LESY ČESKÉ REPUBLIKY, S.P.

[redacted]

ID SML:20250007-LESYCR-001

SMLOUVA O PODPOŘE PROVOZU A ROZVOJE SYSTÉMU DMS

dle ustanovení § 1746 odst. 2, s přihlédnutím k ustanovení § 2358 a násl., jakož i ustanovení § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“)

Lesy České republiky, s.p.
se sídlem Přemyslova 1106/19, Nový Hradec Králové, 500 08 Hradec Králové
IČO: 421 96 451
DIČ: CZ42196451
zapsaný v obchodním rejstříku vedeném Krajským soudem v Hradci Králové, oddíl AXII, vložka 540
zastoupený Ing. Daliborem Šafaříkem, Ph.D., generálním ředitelem
bankovní spojení: Komerční banka, a.s., pobočka Hradec Králové,
č. účtu: 26300511/0100

(dále jako „*objednatel*“) na straně jedné

a

Seyfor, a.s.
se sídlem: Drobného 555/49, 602 00 Brno
IČO: 015 72 377
DIČ: CZ01572377
zapsaná v obchodním rejstříku vedeném u Krajského soudu v Brně, oddíl B, vložka 7072
zastoupená: Martinem Cíglerem, předsedou představenstva
bankovní spojení: Raiffeisenbank a.s.
č. účtu: 6253399002/5500

(dále jako „*dodavatel*“) na straně druhé

(objednatel a dodavatel dále též společně jako „*smluvní strany*“ a každý jednotlivě jako „*smluvní strana*“)

uzavírají níže uvedeného dne, měsíce a roku tuto Smlouvu o podpoře provozu a rozvoje systému DMS (dále jen „*Smlouva*“):

I.
Úvodní ustanovení

1. Objednatel realizoval otevřené řízení dle ustanovení § 56 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, k zadání nadlimitní veřejné zakázky s názvem **„Podpora provozu a rozvoje systému DMS“**, ev. č.: 099/2024/055.

Na základě výsledku zadávacího řízení objednatel rozhodl o podpisu Smlouvy s dodavatelem.

II.
Předmět Smlouvy

1. Dodavatel se Smlouvou zavazuje zajistit objednateli maintenance licencí produktu TS-DATAPOINT (1 ks) a TS-ELDAx (1 ks), poskytování služeb údržby (maintenance) u objednatele implementovaného DMS a poskytování služeb podpory provozu a rozvoje takového DMS, jakož i poskytnout mu oprávnění k výkonu práva užít autorská díla (počítačové programy) vzniklá nebo dodaná při plnění Smlouvy, jež jsou potřebná k řádnému užívání díla (poskytnutého plnění) objednatelem, a to na celou dobu trvání práv autora.
2. Maintenance licencí produktu TS-DATAPOINT (1 ks) a TS-ELDAx (1 ks) dle odstavce 1 tohoto článku Smlouvy zahrnuje údržbu a technickou podporu daného software, zaručuje uživateli nárok na využívání technické podpory a bezplatných upgradů na nové verze.
3. Údržba (maintenance) DMS dle odstavce 1 tohoto článku Smlouvy zahrnuje údržbu (maintenance) software a firmware produktů, které jsou uvedeny v odstavcích 1 a 2 tohoto článku Smlouvy, spočívající zejména v poskytování a implementaci nových verzí těchto produktů, provádění update či upgrade těchto produktů a instalaci opravných patchů. Služba údržby (maintenance) DMS musí zajistit provozuschopnost, spravovatelnost vlastními nástroji a zálohovatelnost DMS, exportovatelnost dat a migrovatelnost dat, aplikací a prostředí.
4. Služby dle odstavců 2 a 3 tohoto článku Smlouvy zahrnují:
   a) servisní podporu v českém anebo slovenském jazyce v režimu 9×5 NBD (následující pracovní den) v pracovních dnech od 08:00 hod. do 17:00 hod., která zahrnuje:
      i. odeslání (nahlášení) požadavku objednatelem,
      ii. přijetí požadavku dodavatelem,
      iii. analýzu problému dodavatelem,
      iv. odstranění závady, vyřešení problému, technického incidentu anebo provedení jiného požadovaného úkonu servisní podpory následující pracovní den v případě odeslání písemného požadavku do 15 hod předcházejícího pracovního dne, v případě, že požadavek bude odeslán později, považuje se za okamžik odeslání požadavku osmá hodina ranní (8:00 hod.) následujícího pracovního dne po odeslání požadavku;
   b) poskytování služeb údržby software, zahrnující zejména poskytování nových verzí software pro update či upgrade software a instalaci opravných patchů;
   c) podporu při konfiguračních změnách, konzultace, profylaxe;
   d) oprava dat na základě požadavku objednatele do 5 pracovních dnů od doručení písemného požadavku objednatele, pokud se smluvní strany nedohodnou jinak.

5. Podpora provozu a rozvoje DMS dle odstavce 1 tohoto článku Smlouvy zahrnuje řešení změnových požadavků (požadavků na rozvoj systému) DMS objednatele, technickou podporu objednatele, jakož i konzultace pracovníkům objednatele, a to prostřednictvím osob podle rolí technik/systémový inženýr, vývojář a architekt/analytik, v českém nebo slovenském jazyce (dále také jen „**Služby rozvoje a podpory**“).

   Postup objednávání **Služeb rozvoje a podpory** spočívajících nikoli pouze v prosté fyzické přítomnosti či konzultaci pracovníka dodavatele je uveden v čl. VI. Smlouvy.

   Předpokládaný a zároveň maximálně možný rozsah poskytování **Služeb rozvoje a podpory** dodavatelem dle Smlouvy činí 2 000 Man-days (člověkodnů). Objednatel negarantuje dodavateli jakýkoliv minimální objem poptávky **Služeb rozvoje a podpory**; takový objem bude vycházet z aktuálních potřeb objednatele. Jeden Man-day činí pro účely Smlouvy 8 celých hodin.

6. Cílem (potřebou), který má být plněním Smlouvy u objednatele naplněn, je (nikoli však výlučně) zajištění funkčnosti a rozvoje u objednatele implementovaného systému DMS, který k okamžiku uzavření Smlouvy zahrnuje agendy: Řízená dokumentace, Centrální registr smluv, Centrální registr objednávek, Technická knihovna, Povolenky a výjimky ze zákazu vjezdu, Účetní doklady, Historie OJ, Veřejné zakázky, Řízení změn, Řízení projektů, Pověření, Personální dokumenty, jakož i zajištění možnosti dalšího rozvoje elektronizace schvalovacích procesů.

7. Při plnění Smlouvy je dodavatel povinen dbát existujících licenčních ujednání týkajících se řešení TS-DATAPOINT a TS-ELDAx, která jsou přílohou č. 1 a č. 2 Smlouvy a Standardů systémové bezpečnosti, které jsou přílohou č. 3 Smlouvy

8. Objednatel se zavazuje poskytnout dodavateli stanovenou součinnost při plnění této Smlouvy.

III.
Doba a místo plnění

1. Plnění dle čl. II. odst. 2 až 4 Smlouvy se dodavatel zavazuje poskytovat objednateli po dobu 3 let ode dne nabytí účinnosti Smlouvy.

2. **Služby rozvoje a podpory** (dle čl. II. odst. 5 Smlouvy) je objednatel u dodavatele oprávněn objednávat po dobu poskytování plnění dle čl. II. odst. 2 až 4 Smlouvy uvedenou v odst. 1 tohoto článku Smlouvy. Dodavatel se zavazuje objednatelem řádně objednané **Služby rozvoje a podpory** objednateli poskytnout

3. Dodavatel je povinen předmět plnění Smlouvy poskytovat v sídle objednatele, nedohodnou-li se smluvní strany jinak. Předmět plnění Smlouvy může být poskytován i vzdáleným přístupem, pokud to jeho povaha umožňuje a není-li nezbytné nebo vhodné výkon takového plnění Smlouvy zajistit on-site.

IV.
Cena

1. Za řádné a včasné poskytování plnění dle čl. II. odst. 2 až 4 Smlouvy náleží dodavateli cena ve výši **179 000 Kč** ročně bez DPH. K uvedené ceně bude připočtena DPH ve výši dle příslušných právních předpisů, vznikne-li povinnost k její úhradě.

   Žádné další částky není v souvislosti s poskytováním plnění dle čl. II. odst. 2 až 4 Smlouvy dodavatel oprávněn objednateli účtovat.

2. Za řádně poskytnuté objednatelem poptané **Služby rozvoje a podpory** (dle čl. II. odst. 5 Smlouvy) náleží dodavateli cena ve výši **9 700 Kč** bez DPH za každý jeden Man-day (člověkoden) účelně strávený poskytnutím takového plnění; v případě **Služeb rozvoje o podpory** spočívajících nikoli pouze v prosté fyzické přítomnosti či konzultaci pracovníka dodavatele náleží dodavateli nejvýše částka odpovídající rozsahu plnění písemně odsouhlaseného objednatelem (časová náročnost splnění požadavku uvedená v popisu splnění požadavku schváleném objednatelem). Za **Služby rozvoje a podpory** bude objednatel dodavateli hradit pouze cenu za skutečně poskytnuté **Služby rozvoje a podpory** (dodavatelem řádně poskytnuté a objednatelem poptané) stanovenou dle jejich skutečného rozsahu. Cena bude účtována v poměrné výši za každou, byť i započatou, čtvrthodinu (15 minut) účelně strávenou poskytnutím všech takových služeb. K uvedené ceně bude připočtena DPH ve výši dle příslušných právních předpisů, vznikne-li povinnost k její úhradě.

3. Smluvní strany sjednávají, že ceny za jednotlivá plnění dle Smlouvy uvedené v odst. 1 a odst. 2 tohoto článku Smlouvy mají charakter cen finálních (maximálně přípustných), tj. zahrnují veškeré náklady spojené s plněním Smlouvy. Dodavatel tak není v souvislosti s plněním Smlouvy oprávněn účtovat a požadovat na objednateli úhradu jakýchkoliv jiných či dalších částek.

V.
Platební podmínky

1. Cena dle čl. IV. odst. 1 Smlouvy bude dodavateli objednatelem hrazena vždy jednou ročně (počítáno od nabytí účinnosti Smlouvy), přičemž dodavatel je oprávněn příslušnou fakturu vystavit nejdříve 2 pracovní dny před zahájením příslušného roku, v němž budou tyto služby poskytovány s výjimkou faktury za 1. rok poskytování těchto služeb, kterou je dodavatel oprávněn vystavit nejdříve dva pracovní dny po nabytí účinnosti Smlouvy.

2. Cena dle čl. IV. odst. 2 Smlouvy bude dodavateli objednatelem hrazena na základě dodavatelem řádně vystavených faktur splňujících náležitosti účetního dokladu a je-li plnění předmětem příslušné daně též náležitosti daňového dokladu dle příslušných obecně závazných právních předpisů, jejíž přílohou bude objednatelem schválený výkaz dle čl. VI. odst. 3 Smlouvy.

3. Splatnost ceny dle odstavců 1 a 2 je 30 dnů od doručení řádně vystavené faktury (daňového dokladu) obsahující veškeré zákonné a smluvené náležitosti, jak předepsáno výše. Nebude-li faktura obsahovat některou stanovenou náležitost, bude-li chybně vyúčtována cena anebo

bude-li faktura obsahovat jinou vadu, je objednatel oprávněn fakturu vrátit dodavateli bez zaplacení (proplacení). Objednatel přitom uvede důvod vrácení.

4. Veškeré cenové údaje podle Smlouvy musí být uvedeny v českých korunách a veškeré platby podle Smlouvy budou prováděny v české měně.
5. Fakturační adresou je adresa sídla objednatele. Dodavatel doručí fakturu v elektronické podobě na adresu [redacted]
6. Cena se považuje za včas uhrazenou, pokud je příslušná částka nejpozději v den splatnosti odepsána z účtu objednatele ve prospěch účtu dodavatele.
7. Dodavatel není oprávněn započíst jakékoliv pohledávky proti nárokům objednatele. Pohledávky a nároky dodavatele vzniklé v souvislosti se Smlouvou nesmí být postoupeny třetím osobám, zastaveny nebo s nimi jinak disponováno. Jakékoliv právní jednání učiněné dodavatelem v rozporu s tímto ustanovením Smlouvy bude považováno za příčící se dobrým mravům.
8. Dodavatel prohlašuje, že v době uzavření Smlouvy není nespolehlivým plátcem ve smyslu ustanovení § 106a zákona č. 235/2004 Sb., o dani z přidané hodnoty, v účinném znění a zavazuje se, že v případě, že se v době plnění Smlouvy takovým nespolehlivým plátcem stane, oznámí tuto skutečnost neprodleně písemně objednateli.
9. Bude-li dodavatel ke dni poskytnutí zdanitelného plnění veden jako nespolehlivý plátce ve smyslu ustanovení § 106a zákona č. 235/2004 Sb., o dani z přidané hodnoty, v účinném znění, je objednatel oprávněn část ceny odpovídající DPH uhradit přímo na účet správce daně; dodavatel v takovém případě obdrží pouze cenu bez DPH.

VI.
Postup při objednávání a poskytování Služeb rozvoje a podpory a výkaz

1. Na základě písemného požadavku na poskytnutí **Služeb rozvoje a podpory** (dle čl. II. odst. 5 Smlouvy) spočívajících nikoli pouze v prosté fyzické přítomnosti či konzultaci pracovníka dodavatele, vzneseného objednatelem, má dodavatel povinnost provést a předložit objednateli popis splnění požadavku, a to včetně popisu způsobu splnění. V popisu bude uveden možný dopad splnění požadavku do zájmů objednatele, harmonogram prací nutných ke splnění požadavku s časovým vytížením jednotlivých rolí (časovou náročností splnění požadavku) a garantovaná doba splnění požadavku, počítaná od odsouhlasení popisu splnění požadavku objednatelem. Popis splnění požadavku splňující shora uvedené náležitosti dodavatel doručí objednateli k odsouhlasení nejpozději do 5 pracovních dní od jeho zaslání objednatelem na Helpdesk e-mail nebo Servicedesk web dodavatele dle Smlouvy a po písemném odsouhlasení popisu objednatelem požadavek v souladu se schváleným popisem splní. V případě nedohody je objednatel oprávněn od Smlouvy odstoupit.
2. O poskytnutí **Služeb rozvoje a podpory** dodavatel zpracuje výkaz, a to vždy zpětně za uplynulý kalendářní měsíc. Výkaz bude obsahovat popis plnění poskytnutých dodavatelem objednateli v rámci těchto služeb v uplynulém kalendářním měsíci, tak, aby žádné nemohlo

být zaměněno za jiné, včetně datumu, kdy bylo každé takové plnění poskytnuto, spolu s dobou účelně dodavatelem vynaloženou na poskytnutí takového plnění v minutách, jakož i s uvedením jména a příjmení pracovníka (jmen a příjmení pracovníků) dodavatele, který plnění poskytl (kteří plnění poskytli). Výkaz předloží dodavatel objednateli ke kontrole a schválení.

3. Osoba oprávněná jednat za objednatele ve věcech technických bez zbytečného odkladu zkontroluje předložený výkaz. Pokud bude výkaz bezchybný, schválí ho, což provede na výkaz svým podpisem.
4. Schválený výkaz je podkladem k vystavení faktury dle čl. V. odst. 2 Smlouvy.

VII.
Další práva a povinnosti smluvních stran

1. Při plnění Smlouvy je dodavatel oprávněn jednat se všemi kompetentními zaměstnanci objednatele za účelem zajištění transparentního a efektivního průběhu procesu poskytování smluvených plnění. Dodavatel je oprávněn požadovat po kompetentních osobách objednatele součinnost nezbytnou pro plnění Smlouvy.
2. Dodavatel je povinen plnit Smlouvu řádně, včas a s nejvyšší odbornou péčí. Při plnění Smlouvy dodavatel spolupracuje s osobami oprávněnými jednat za objednatele ve věcech technických, pravidelně je informuje o plnění Smlouvy a řídí se jejich pokyny. Ustanovení § 2594 občanského zákoníku platí obdobně.
3. Dodavatel je povinen plnit Smlouvu v souladu s obecně závaznými právními předpisy i zvláštními právními předpisy vztahujícími se k předmětu plnění Smlouvy, zejména v souladu se zákonem č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů, zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů, zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů a Nařízením Evropského parlamentu a Rady (EU) 2016/679.
4. Dodavatel je dále povinen, nedohodnou-li se smluvní strany předem jinak, při plnění Smlouvy dodržovat obecně platné standardy, zejména:

    - RFC
    - CIS (Center for Internet Security Benchmark)
    - OWASP
    - ISO/IEC 2700x (ISMS)
    - ISO/IEC 12207 (*Systems and software engineering – Software life cycle processes*)
    - ISO/IEC 15504 *(Software Process Improvement and Capability Determination (SPICE)).*

5. Dodavatel má povinnost realizovat předmět Smlouvy tak, aby na serverech vztahujících se k předmětu plnění Smlouvy byly nainstalovány a byly v provozu pouze takové služby, které jsou nezbytné pro korektní běh aplikací nebo správy systému DMS.

6. Dodavatel má povinnost používat v rámci realizace předmětu plnění Smlouvy pouze služby či protokoly, které vyhovují bezpečnostním požadavkům pro přenos či zpracování informací dle příslušné kategorie jejich citlivosti; za nevyhovující je považováno zejména:

    - použití nešifrovaných protokolů pro vzdálenou administraci (TELNET, http atd.),
    - použití nešifrovaných protokolů pro přenos dat (FTP http atd.),
    - použití slabých a již nevyhovujících metod šifrování (SSL2, SSL3, SHA1 atd.),
    - použití zranitelných protokolů RDP, IMAP,
    - použití služeb se známou zranitelností, která není výrobcem opravena nebo je neopravitelná,
    - použití služeb bez podpory výrobce (Out Of Life).

VIII.
Mlčenlivost

1. Dodavatel se zavazuje zachovávat mlčenlivost o všech informacích týkajících se objednatele nebo Smlouvy či jejího plnění, které (a) získal přímo či nepřímo od objednatele v souvislosti s uzavřením anebo plněním Smlouvy anebo (b) je získá jiným způsobem v souvislosti s plněním Smlouvy (dále jen „důvěrné informace“). Povinnost mlčenlivosti zahrnuje povinnost dodavatele učinit vše, co lze spravedlivě požadovat, aby důvěrné informace nevešly ve známost nepovolané osoby.

2. Dodavatel je oprávněn sdělit důvěrnou informaci třetí osobě pouze s předchozím písemným souhlasem objednatele s tím, že tento souhlas je vázán na povinnost zavázat tuto třetí osobu, aby nakládala s těmito informacemi jako s důvěrnými a na souhlas této třetí osoby, že závazek přijímá, a to alespoň v rozsahu stanoveném Smlouvou; tím nejsou dotčeny povinnosti dodavatele stanovené obecně závaznými právními předpisy.

3. Důvěrnými informacemi nejsou nebo přestávají být:

    a) informace, které byly v době, kdy je dodavatel získal, veřejně známé, nebo

    b) informace, které je dodavatel povinen sdělit oprávněné osobě na základě účinných právních předpisů.

4. Poskytnutí informace na základě povinnosti stanovené dodavateli obecně závazným právním předpisem není považováno za porušení povinnosti dodavatele sjednané v tomto článku Smlouvy. Jedná se zejména o povinnost na žádost poskytnout informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů či zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, či jiných obecně závazných právních předpisů.

IX.
Komunikace smluvních stran

1. Smluvní strany se zavazují při plnění této Smlouvy komunikovat prostřednictvím Servicedesk webu (viz odst. 2 tohoto článku smlouvy), který musí být dostupný 24 hodin denně, 7 dní v týdnu. V odůvodněných případech, zejména v případě nefunkčnosti Servicedesk webu nebo v případě vad plnění Smlouvy, jsou smluvní strany oprávněny komunikovat prostřednictvím Helpdesk e-mailu, Helpdesk telefonu (viz odst. 2 tohoto článku smlouvy) nebo prostřednictvím kontaktních osob (viz odst. 4 a odst. 5 tohoto článku Smlouvy).

2. Adresy (kontaktní údaje) dodavatele, na něž je objednatel oprávněn doručit dodavateli příslušný požadavek, popř. nahlásit závadu dodavateli:

   Servicedesk web: [redacted]

   Helpdesk e-mail: [redacted]

   Helpdesk telefon: [redacted]

3. Dodavatel se zavazuje zajistit dostupnost ServiceDesk webu alespoň z 95 % doby trvání každého kalendářního měsíce. Objednatel předpokládá údržbu Servicedesk webu, přičemž Dodavatel je povinen Objednatele o nedostupnosti Servicedesk webu z důvodu jeho plánované údržby písemně informovat min. 48 hodin předem. Nedostupnost Servicedesk webu po dobu jeho údržby se započítává do doby jeho nedostupnosti ve smyslu věty první tohoto odstavce.

   Požadavky objednatele doručené dodavateli telefonicky je dodavatel povinen písemně (e-mailem) objednateli potvrdit a zaevidovat na Servicedesk webu.

4. Osoby oprávněné zastupovat objednatele v technických záležitostech týkajících se Smlouvy (kontaktní osoby):

   [redacted]

   [redacted]

5. Osoba/osoby oprávněná/oprávněné zastupovat dodavatele v technických záležitostech týkajících se Smlouvy (kontaktní osoba/osoby):

   [redacted]

6. Každá ze smluvních stran je oprávněna své kontaktní osoby a/nebo jejich kontaktní údaje jednostranně změnit, a to prostřednictvím písemného oznámení doručeného druhé smluvní straně. Změna je účinná okamžikem doručení oznámení druhé smluvní straně.

X.
Odpovědnost za škodu

1. Odpovědnost smluvních stran za škodu se řídí ustanovením § 2894 a násl. občanského zákoníku. Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k jejich minimalizaci.
2. Dodavatel je povinen za objednatele úplně a bez přispění objednatele vyřídit a urovnat jakékoli oprávněné požadavky třetích osob vyplývající z případných autorských práv (jejich možného porušení atp.) k předmětu plnění Smlouvy.
3. Smluvní strana neodpovídá za újmu, která vznikla v důsledku věcně nesprávného nebo jinak chybného zadání, které obdržela od druhé smluvní strany.
4. Smluvní strana není odpovědná za újmu způsobenou prodlením druhé smluvní strany s jejím vlastním plněním Smlouvy.
5. Smluvní strany se zavazují upozornit druhou smluvní stranu bez zbytečného odkladu na vzniklé okolnosti vylučující odpovědnost bránící řádnému plnění této Smlouvy.

XI.
Smluvní pokuty

1. V případě prodlení dodavatele s odstraněním závady, vyřešením problému, technického incidentu anebo provedením jiného požadovaného úkonu servisní podpory (viz čl. II. odst. 4 Smlouvy) je dodavatel povinen objednateli uhradit smluvní pokutu ve výši 3 000 Kč za každý, byť i započatý kalendářní den prodlení.
2. V případě prodlení dodavatele s doručením řádného popisu splnění požadavku objednateli (viz čl. VI. odst. 2 Smlouvy) je dodavatel povinen objednateli uhradit smluvní pokutu ve výši 3 000 Kč za každý, byť i započatý kalendářní den prodlení.
3. V případě že dodavatel nedodrží dobu splnění požadavku uvedenou v objednatelem odsouhlaseném popisu splnění požadavku (viz čl. VI. odst. 2 Smlouvy), je dodavatel povinen objednateli uhradit smluvní pokutu ve výši 3 000 Kč za každý, byť i započatý kalendářní den prodlení.
4. Ujednáním o smluvní pokutě, uplatněním práva na její zaplacení ani jejím zaplacením není, a to ani zčásti, dotčen nárok objednatele na náhradu škody.
5. Smluvní strany prohlašují, že sjednaná výše smluvních pokut je přiměřená významu zajištěné/utvrzené právní povinnosti.
6. Smluvní pokuty mohou být kombinovány (tzn., že uplatnění jedné smluvní pokuty nevylučuje uplatnění jakékoliv jiné smluvní pokuty), nestanoví-li Smlouva jinak.
7. Vznikem povinnosti dodavatele zaplatit smluvní pokutu ani jejím samotným zaplacením nezaniká povinnost dodavatele splnit povinnost, jejíž splnění bylo smluvní pokutou zajištěno. Dodavatel je i nadále povinen ke splnění takovéto povinnosti.

8. Smluvní pokuta je splatná do 21 dnů od doručení písemného oznámení o jejím uplatnění dodavateli.
9. Objednatel je oprávněn svou pohledávku, splatnou i nesplatnou, za dodavatelem z titulu povinnosti dodavatele zaplatit smluvní pokutu započíst oproti pohledávce dodavatele za objednatelem z titulu povinnosti objednatele zaplatit cenu dle čl. IV. Smlouvy.
10. Pro případ prodlení s úhradou peněžitého závazku dle Smlouvy je smluvní strana, která je v prodlení, povinna zaplatit druhé smluvní straně úrok z prodlení ve výši 0,05 % z dlužné částky za každý, byť i započatý den prodlení.

XII.
Odstoupení od Smlouvy

1. Kterákoli ze smluvních stran je oprávněna od Smlouvy písemně odstoupit v případech a za podmínek stanovených občanským zákoníkem a/nebo ujednaných Smlouvou.
2. Objednatel je oprávněn od Smlouvy písemně odstoupit zejména v případě, že
   a) se dodavatel ocitl v prodlení s odstraněním závady, vyřešením problému, technického incidentu anebo provedením jiného požadovaného úkonu servisní podpory o dobu delší než 30 kalendářních dnů;
   b) se dodavatel ocitl v prodlení s doručením řádného popisu splnění požadavku objednateli (dle čl. VI. odst. 2 Smlouvy) o dobu delší než 20 kalendářních dnů;
   c) se dodavatel ocitl v prodlení se splněním požadavku dle objednatelem odsouhlaseného popisu splnění požadavku (dle čl. VI. odst. 2 Smlouvy) o dobu delší než 30 kalendářních dnů;
   d) dodavatel vstoupil do likvidace;
   e) nabylo právní moci rozhodnutí soudu o úpadku dodavatele ve smyslu zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů;
   f) z chování či jednání dodavatele lze mít za to, že Smlouvu poruší podstatným způsobem.
3. Dodavatel je oprávněn od Smlouvy písemně odstoupit zejména v případě, že se objednatel ocitl v prodlení se zaplacením ceny dle Smlouvy o dobu delší než 30 kalendářních dnů.
4. V případě odstoupení od Smlouvy jsou smluvní strany povinny vypořádat své vzájemné závazky a pohledávky vyplývající z této Smlouvy do 30 kalendářních dnů od právních účinků odstoupení.
5. Předčasným ukončením Smlouvy není dotčena platnost kteréhokoliv ustanovení Smlouvy, jež má výslovně či ve svých následcích zůstat v platnosti po jejím zániku. Předčasné ukončení Smlouvy se nedotýká práva na zaplacení smluvní pokuty, dospělého úroku z prodlení, práva na náhradu škody vzniklé z porušení smluvní povinnosti ani ujednání, které má vzhledem ke

své povaze zavazovat smluvní strany i po ukončení Smlouvy, zejména závazku mlčenlivosti a ochrany informací, zajištění a utvrzení závazků a ujednání o způsobu řešení sporů.

XIII.
Záruka a uplatnění práv z odpovědnosti za vady

1. Dodavatel poskytuje objednateli záruku za jakost na služby uvedené v čl. II Smlouvy o době trvání 24 měsíců. Záruka začíná běžet dnem převzetí služby.

2. Dodavatel je povinen bez zbytečného odkladu po obdržení oznámení vady písemně oznámit objednateli, zda vadu služby uznává či neuznává. Pokud tak neučiní, platí, že vadu uznává. Neuplatní-li objednatel písemně při oznámení vady jiné právo z odpovědnosti za vady, platí, že požaduje odstranění vady. Vadu je dodavatel povinen odstranit nejpozději do 30 dnů od jejího oznámení objednatelem, nebude-li smluvními stranami písemně ujednáno jinak.

XIV.
Závazek a prohlášení dodavatele

1. Dodavatel se zavazuje:

   a) po celou dobu trvání smluvního vztahu založeného Smlouvou zajistit především důstojné pracovní podmínky pro veškeré své zaměstnance podílející se na plnění Smlouvy, stejně jako udržovat férové dodavatelské vztahy s obchodními partnery, jejichž služeb při plnění Smlouvy využije,

   b) dodržovat veškeré právní předpisy, zejména pak z oblasti práva životního prostředí, práva sociálního či pracovního (odměňování, dodržování délky pracovní doby a doby odpočinku mezi směnami, placené přesčasy), dále předpisy týkající se oblasti zaměstnanosti a bezpečnosti a ochrany zdraví při práci, tj. zejména zákon č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů, a zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů, a to vůči všem osobám či subjektům, které se na plnění Smlouvy podílejí a bez ohledu na to, zda bude plnění poskytováno jím samotným či jeho poddodavatelem. Dodavatel zajistí, že na plnění smlouvy se budou podílet pouze osoby, které byly proškoleny z problematiky BOZP a požární ochrany, a jsou náležitě vybaveny osobními ochrannými pracovními prostředky dle účinné legislativy. Současně je dodavatel povinen dodržovat veškeré podmínky, které ujednal se svými obchodními partnery podílejícími se na plnění Smlouvy, zejména je vůči nim povinen řádně a včas plnit své finanční závazky při respektování ustanovení § 1963 občanského zákoníku.

2. Dodavatel prohlašuje, že veřejný funkcionář uvedený v ustanovení § 2 odst. 1, písm. c) zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů, nebo jím ovládaná osoba nevlastní v dodavateli ani v žádné z osob, jejichž prostřednictvím dodavatel v zadávacím řízení na výběr dodavatele prokazoval kvalifikaci, podíl představující alespoň 25 % účasti společníka. V případě, že prohlášení dodavatele učiněné v předchozí větě je nebo se ukáže být nepravdivým, je objednatel oprávněn od Smlouvy písemně odstoupit.

3. Dodavatel prohlašuje, že ke dni uzavření Smlouvy u něj neexistují podmínky pro uplatnění mezinárodních sankcí ve smyslu § 48a zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, a současně se zavazuje, že tyto nebudou existovat ani po celou dobu účinnosti Smlouvy; v opačném případě je objednatel oprávněn od Smlouvy písemně odstoupit.

XV.
Criminal Compliance doložka

1. Smluvní strany níže svým podpisem stvrzují, že v průběhu vyjednávání o Smlouvě vždy jednaly a postupovaly čestně, transparentně a v souladu s veškerými právními předpisy, a že takto budou jednat i při jejím plnění.
2. Smluvní strany prohlašují, že v souvislosti se Smlouvou vyvinou maximální úsilí, aby žádné ze smluvních stran nemohla být přičtena trestní odpovědnost podle příslušných právních předpisů.
3. Objednatel zachovává nulovou toleranci k jakémukoli nelegálnímu jednání, dodržuje maximální transparentnost, legalitu, etiku a uplatňuje zásady Criminal Compliance Programu (www.lesycr.cz/ccp).

XVI.
Závěrečná ustanovení

1. Smlouva nabývá platnosti dnem jejího podpisu oběma smluvními a účinnosti nabývá dnem jejího uveřejnění v registru smluv dle ustanovení § 6 zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů.
2. Pokud není ve Smlouvě ujednáno jinak, řídí se vztahy mezi smluvními stranami právním řádem České republiky, zejména občanským zákoníkem a právními předpisy souvisejícími.
3. Tuto Smlouvu lze měnit či doplňovat pouze formou písemných dodatků podepsaných oběma smluvními stranami.
4. Veškeré spory vzniklé ze Smlouvy, které se nepodaří přednostně vyřešit smírně, budou rozhodovány obecnými soudy České republiky a v souladu se zákonem č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů.
5. Pokud některé z ustanovení Smlouvy je nebo se stane neplatným, neúčinným či zdánlivým, neplatnost, neúčinnost či zdánlivost tohoto ustanovení nebude mít za následek neplatnost Smlouvy jako celku ani jiných ustanovení Smlouvy, pokud je takovéto ustanovení oddělitelné od zbytku Smlouvy. Smluvní strany se zavazují, bude-li to možné, takovéto neplatné, neúčinné či zdánlivé ustanovení nahradit novým platným a účinným ustanovením, které svým obsahem bude co nejvěrněji odpovídat podstatě a smyslu původního ustanovení.
6. Žádná ze smluvních stran není oprávněna bez předchozího písemného souhlasu druhé smluvní strany převést na třetí osobu jakákoli práva nebo povinnosti vyplývající ze Smlouvy nebo

postoupit na třetí osobu jakoukoli pohledávku nebo dluh vzniklý na základě Smlouvy včetně práv, povinností, pohledávek nebo dluhů vzniklých na základě porušení Smlouvy. Toto omezení nakládání s právy, povinnostmi, pohledávkami a dluhy trvá i po ukončení Smlouvy. Jakékoliv právní jednání učiněné kteroukoli ze smluvních stran v rozporu s tímto omezením bude považováno za příčící se dobrým mravům.

7. Dodavatel bere na vědomí, že objednatel bude postupovat v souladu se svými povinnostmi stanovenými v zákoně č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, a uveřejní na svém profilu zadavatele údaje a dokumenty, k jejichž uveřejnění je dle zmíněného zákona povinen. Dodavatel souhlasí s uveřejněním Smlouvy a výše skutečně uhrazené ceny na základě Smlouvy. Dále dodavatel bere na vědomí, že objednatel bude postupovat v souladu s povinnostmi stanovenými dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů, a uveřejní Smlouvu v registru smluv.
8. Zastupuje-li každou ze smluvních stran osoba oprávněná za ni jednat, jež disponuje platným uznávaným elektronickým podpisem ve smyslu zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů, je Smlouva uzavírána elektronicky. V ostatních případech se Smlouva uzavírá v listinné podobě a je vyhotovena v počtu 4 stejnopisů, z nichž po 2 vyhotoveních obdrží každá ze smluvních stran.
9. Smluvní strany prohlašují, že si Smlouvu před jejím podpisem přečetly, jejímu obsahu rozumí a bez výhrad s ním souhlasí. Smlouva je vyjádřením jejich pravé, skutečné, svobodné a vážné vůle, na důkaz čehož níže připojují, prosty omylu, své podpisy.
10. Nedílnou součástí Smlouvy jsou tyto její přílohy:
    - Příloha č. 1 – Licenční ujednání týkajících se řešení TS-DATAPOINT
    - Příloha č. 2 – Licenční ujednání týkající se řešení TS-ELDAx
    - Příloha č. 3 – Standard systémové bezpečnosti

V Hradci Králové, dne *elektronického podpisu*

……
Ing. Dalibor Šafařík, Ph.D.
generální ředitel
Lesy České republiky, s.p.

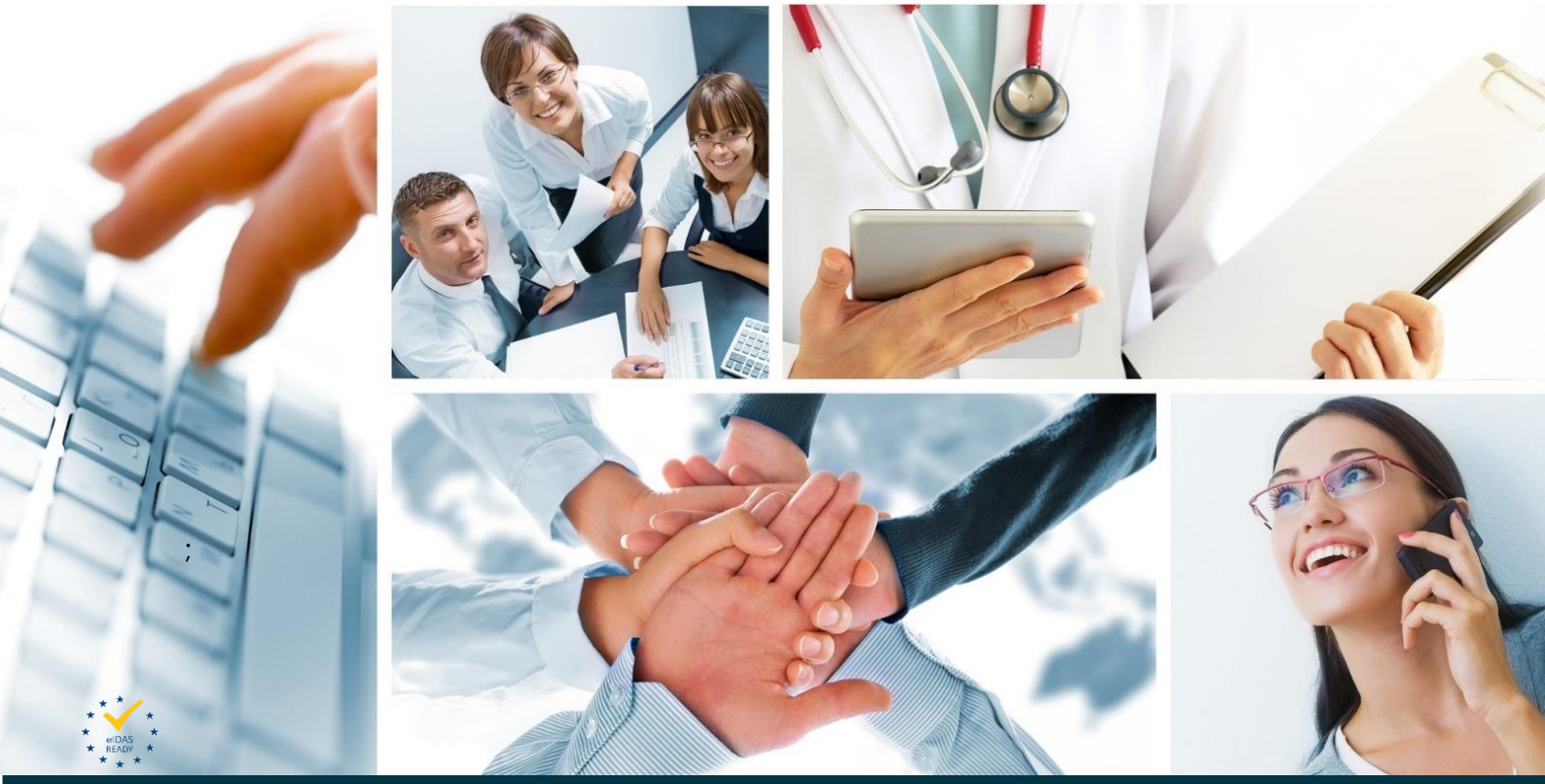
V Brně, dne dle *elektronického podpisu*

……
Martin Cígler
předseda představenstva
Seyfor, a.s.

ELDAx Seyfor

eIDAS SMART TRUST eLECTRONIC PLATFORM

LICENČNÍ PODMÍNKY SW PRODUKTU TS-DATAPOINT



GO DIGITAL

ELDAx.cz

Označení dokumentu	**Licenční podmínky**	**STÁDIUM:**	**Schváleno**
		DŮVĚRNOST:	Veřejné
ZE DNE:	1. 1. 2016	**DATUM AKTUALIZACE:**	1. 1. 2023
ZPRACOVAL / AUTOR:	Luděk Telecký	**VERZE DOKUMENTU:**	3.0

1. Úvodní ustanovení

1.1. Tyto licenční podmínky jsou závazné pokyny pro Nabyvatele práv užití softwarového produktu o způsobu, možnostech a právech užití softwarového produktu (dále jen LICENČNÍ PODMÍNKY) – softwarového produktu – určené pro práci s elektronickými dokumenty:

TS-DATAPOINT

1.2. Softwarový produkt TS-DATAPOINT je řešení určené pro správu a oběh (workflow) dokumentů v rámci organizace. TS-DATAPOINT obsahuje celý soubor vzájemně propojených agend pokrývající všechny standardní procesy organizace. Agendy TS-DATAPOINT pokrývají klíčové procesy společnosti, a jsou určeny pro implementaci do prostředí technologie MS SharePoint různých verzí. Nabytí licence TS-DATAPOINT je samostatný právní akt a jakkoliv neovlivňuje nebo nepodmiňuje způsob licencování prostředí MS-SharePoint Nabyvatelem licence.

1.3. TS-DATAPOINT je složen agend, obsahuje uživatelskou dokumentaci v elektronické formě, a může obsahovat další materiály v tištěné či elektronické podobě. Pro účely těchto LICENČNÍCH PODMÍNEK se pro soubor těchto položek a materiálů zahrnutých v softwarovém produktu používá jednotné označení TS-DATAPOINT.

1.4. Nabyvatel je oprávněn k užívání TS-DATAPOINT v rozsahu stanoveném těmito Licenčními Podmínkami. Licence podle těchto PODMÍNEK neopravňuje Nabyvatele k jakémukoli jinému nakládání s TS-datapoint, než je upraveno těmito LICENČNÍMI PODMÍNKAMI nebo než vyplývá z platných právních předpisů.

1.5. Okamžikem nabytí se pro účely použití Licence produktu TS-DATAPOINT rozumí datum zdanitelného plnění uvedené na daňovém dokladu vystaveného dodavatelským subjektem. V případě neexistence takového dokladu, může tento dokument nahradit jiný doklad, jednoznačně určující datum předání/převzetí Licence TS-DATAPOINT Nabyvatelem.

Majitel autorských práv

1.6. Majitelem všech autorských práv k produktu TS-DATAPOINT je společnost Seyfor,

a.s. Okružní 5, BRNO, ČESKÁ REPUBLIKA, IČ 01572377, spisová značka: B 7072 vedená u Krajského soudu v Brně.

2. Licence k softwarovému produktu TS-DATAPOINT

2.1. Licence TS-DATAPOINT obsahuje tato práva užití:

2.1.1. Přístup z klientských zařízení: TS-DATAPOINT může být na zařízení prostřednictvím klientské aplikace používán k běžnému užití – tj. může být spouštěn, prohlížena, vkládána nebo měněna v něm pomocí klientské aplikace data či je možné data jiným způsobem užívat na neomezeném počtu zařízení používaných zaměstnanci Nabyvatele. Toto ustanovení se vztahuje na všechna Zařízení, která technologicky umožňují instalaci klientské aplikace. Zařízením se rozumí server, počítač, pracovní stanice, terminál, PDA, zařízení typu „inteligentní telefon“ nebo jiné elektronické digitální zařízení, na kterém je možné pomocí klienta přistupovat k TS-DATAPOINT. Zařízení jako takové nemusí být ve vlastnictví Nabyvatele, ale osoba Používající toto zařízení musí být zaměstnancem Nabyvatele, pokud nesplňuje některou z podmínek níže.

2.1.2. PRODUKČNÍ SERVEROVÁ LICENCE (PROSERVER): Licence opravňuje instalovat a používat jednu kopii TS-DATAPOINT pro produkční provoz Nabyvatele. Licence neopravňuje k instalaci TS-DATAPOINT současně na více Zařízeních.

2.1.3. TESTOVACÍ SERVEROVÁ LICENCE (TESTSERVER): Licence opravňuje instalovat jednu kopii TS-DATAPOINT do testovacího prostředí Nabyvatele a může být použita výhradně pro "Testovací Provoz". "Testovací provoz" je realizován nad testovacími daty, tedy neúplnými daty z pohledu komplexity a určenými zejména k realizaci testovacích scénářů a má za cíl prověřit funkcionality TS-DATAPOINT. V rámci " Testovacího provozu" může Nabyvatel prověřovat zejména soulad uživatelských vlastností TS-DATAPOINT nebo integrovaných systémů - aplikací. Výstupy jakýchkoliv testovacích činností nesmějí být použity pro jiné účely, než optimalizace nastavení TS-DATAPOINT nebo integrovaných aplikací s TS-DATAPOINT.

2.1.4. ŠKOLÍCÍ SERVEROVÁ LICENCE (EDUSERVER): Licence opravňuje instalovat jednu kopii TS-DATAPOINT do školícího prostředí Nabyvatele. Nabyvatel ve školícím prostředí zvyšuje úroveň ovládání a poznání TS-DATAPOINT pro uživatele nebo administrátory. Výstupy jakýchkoliv školících činností a instalace EDUSERVER nesmějí být použity pro jiné účely, než zvyšování znalosti uživatelů nebo administrátorů TS-DATAPOINT.

2.1.5. ŠKOLÍCÍ SERVEROVÁ LICENCE (EDUSERVER): Licence opravňuje instalovat jednu kopii TS-DATAPOINT do školícího prostředí Nabyvatele. Nabyvatel ve školícím prostředí zvyšuje úroveň ovládání a poznání TS-DATAPOINT pro uživatele nebo administrátory. Výstupy jakýchkoliv školících činností a instalace EDUSERVER

nesmějí být použity pro jiné účely, než zvyšování znalosti uživatelů nebo administrátorů TS-DATAPOINT.

2.1.6. AFILACE LICENCE: Opravňuje k užití TS-DATAPOINT zaměstnanci jedné jiné fyzické či právnické osoby, která je ve vztahu afilace k vlastníkovi licence. AFILAČNÍ LICENCE neopravňuje k instalaci další instance TS-DATAPOINT. Afilací ve smyslu těchto LICENČNÍCH PODMÍNEK se rozumí vztah mezi oprávněným z licence a kteroukoliv právnickou osobou, kterou vlastní, která vlastní jeho nebo je s ním společně vlastněna. Vlastnictví pro účely této definice znamená větší než 50% přímý nebo přepočtený majetkový podíl na právnické osobě.

2.2. Žádná licence TS-DATAPOINT, není určena k:

2.2.1. pronájmu,

2.2.2. sdílení,

2.2.3. poskytování sublicencí jiným subjektům (právnické nebo fyzické osobě),

2.2.4. k využití třetími osobami, s výjimkou případů, kdy třetí osoba zajišťuje provozní potřeby Nabyvatele nebo splňuje podmínky afilace a její přístup je pokryt udělenou AFILAČNÍ LICENCÍ.

2.3. PŘEVOD LICENCE: Veškerá práva a povinnosti vyplývající z těchto LICENČNÍCH PODMÍNEK může Nabyvatel postoupit na nový subjekt pouze po předchozím písemném souhlasu společnosti TECHNISERV IT. V případě udělení souhlasu pro převod licence musí Nabyvatel převést na nový subjekt licence veškeré části TS-DATAPOINT (včetně všech rozšiřujících licencí, médií, tištěného materiálu a aktuální verze Smlouvy na základě které byla licence pořízena) a ze svých Zařízení zcela odstranit všechny instance TS-DATAPOINT nebo jeho Agend. Předpokladem možnosti převodu je i písemný souhlas nového subjektu s realizací převodu a s těmito LICENČNÍMI PODMÍNKAMI.

2.4. Reverzní inženýrství za cílem analýzy TS-DATAPOINT nebo jeho Agend: Nabyvatel nesmí jakkoli využít znalosti o myšlenkách, postupech, struktuře, algoritmu a použitých metodách, na nichž je TS-DATAPOINT založen nebo které obsahuje, i když je získal při oprávněném užití TS-DATAPOINT, vyjma jejich nezbytného užití k dosažení vzájemného funkčního propojení TS-DATAPOINT s jinými počítačovými programy pomocí Standardního Integračního Rozhraní TS-DATAPOINT. Ale ani tyto znalosti nesmí být využity ani k vývoji, zhotovení nebo k obchodnímu využití jiného počítačového programu, ani k jinému jednání ohrožujícímu nebo porušujícímu autorské právo k TS-DATAPOINT. O znalostech získaných při integračních činnostech je Nabyvatel povinen zachovávat mlčenlivost vůči třetím osobám.

2.5. Licence TS-DATAPOINT a Agend se uděluje výhradně na produkt v kompilovaném tvaru

3. Ochranné známky TS-DATAPOINT

3.1. Tyto LICENČNÍ PODMÍNKY neudělují Nabyvateli žádná práva ve spojení s ochrannými známkami TS-DATAPOINT.

4. Ukončení licence a práva k užití TS-DATAPOINT

4.1. V případě porušení těchto LICENČNÍCH PODMÍNEK Nabyvatelem licence zaniká právo Nabyvateli na užívání licence. Tímto ustanovením nezaniká povinnost Nabyvatele uhradit vlastníkovi autorských práv k TS-DATAPOINT za neoprávněné užití licence a zároveň nezaniká náhrada na úhradu vzniklé škody.

4.2. V případě ukončení práva užití TS-DATAPOINT na základě těchto LICENČNÍCH PODMÍNEK končí veškerá práva užití TS-DATAPOINT vč. jeho Agend poskytnutá Nabyvateli. V takovém případě musí Nabyvatel nejpozději v den ukončení práva užití TS-DATAPOINT ze všech svých počítačů zcela odstranit všechny instalace TS-DATAPOINT a jeho Agend.

5. Závěrečná ustanovení

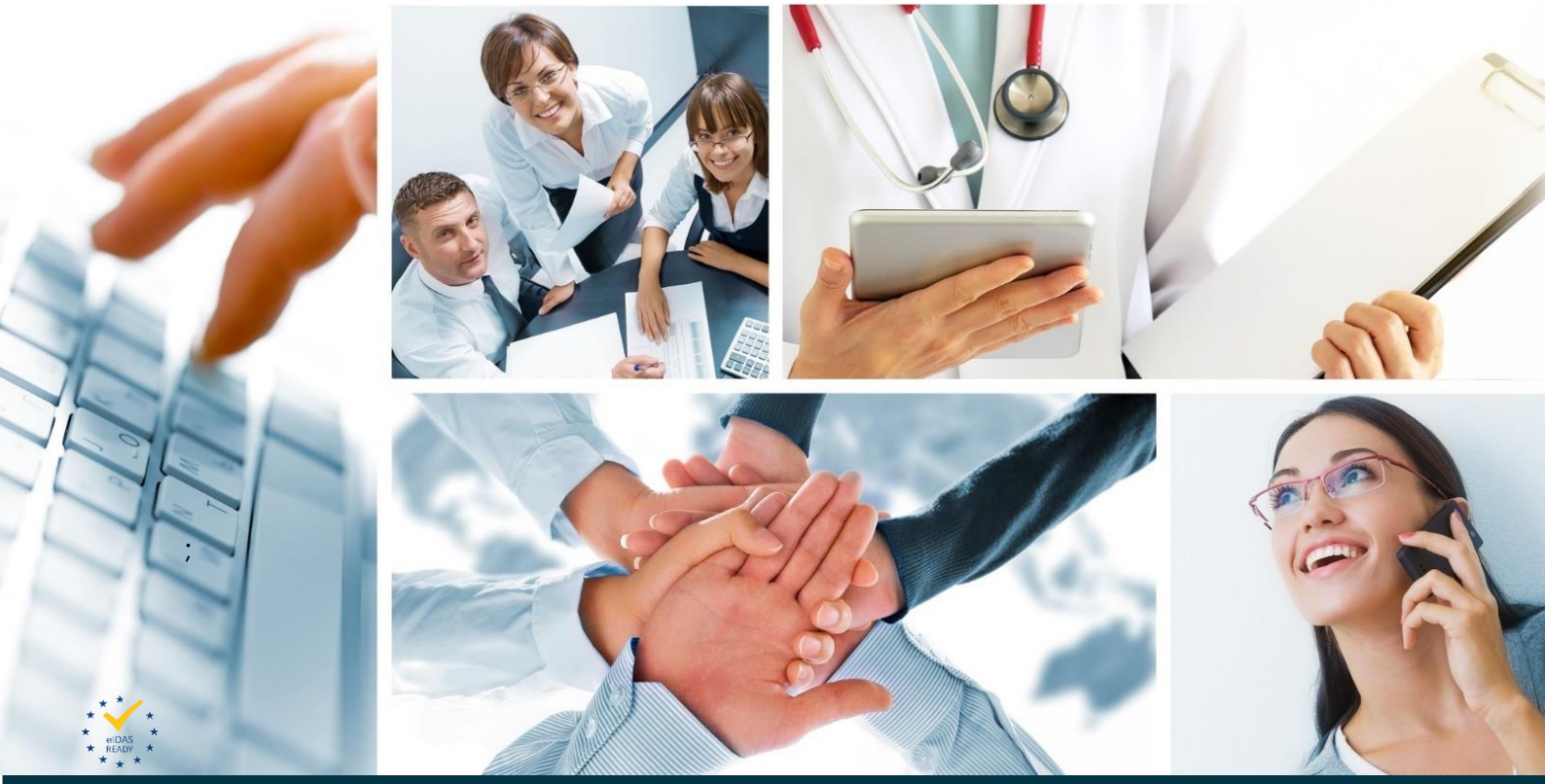
5.1. Tyto licenční podmínky jsou platné od 1. 1. 2016 a nahrazují předchozí „LICENČNÍ PODMÍNKY SOFTWAROVÉHO ŘEŠENÍ TS-DATAPOINT“.

5.2. Pokud soud rozhodne, že některé z ustanovení těchto Licenčních podmínek jsou neplatné, zůstávají zbývající ustanovení platná a účinná.

ELDAx Seyfor

eIDAS SMART TRUST eLECTRONIC PLATFORM

LICENČNÍ PODMÍNKY



GO DIGITAL

ELDAx.cz

Označení dokumentu	**Licenční podmínky**	**STÁDIUM:**	**Schváleno**
Release ELDAx	Po datu platnosti	**DŮVĚRNOST:**	Veřejné
ZE DNE:	1. 1. 2023	**DATUM AKTUALIZACE:**	1. 1. 2023
ZPRACOVAL / AUTOR:	Nicolas Kovařík	**VERZE DOKUMENTU:**	3.0

1. Úvod

1.1. Tyto licenční podmínky jsou závazné pokyny pro Nabyvatele práv užití softwarového produktu o způsobu, možnostech a právech užití softwarového produktu (dále jen LICENČNÍ PODMÍNKY) - softwarové aplikace – určené pro elektronickou důvěryhodnou archivaci s obchodním názvem:

ELDAx eIDAS SMART TRUST eLECTRONIC PLATFORM

1.2. Softwarový produkt ELDAx eIDAS SMART TRUST eLECTRONIC PLATFORM určený pro realizaci procesů a služeb spojených s nařízením eIDAS zahrnuje mimo jiné samotné aplikace v kompilovaném tvaru, případně jejich souvisejících modulů, uživatelskou dokumentaci v elektronické formě a může obsahovat další materiály v tištěné či elektronické podobě.

1.3. Pro účely těchto Licenčních podmínek se pro soubor těchto položek a materiálů zahrnutých v softwarovém produktu používá jednotné označení ELDAx.

1.4. Nabyvatel je oprávněn k užívání ELDAx v rozsahu stanoveném těmito Licenčními podmínkami. Licence podle těchto podmínek neopravňuje Nabyvatele k jakémukoli jinému nakládání s ELDAx, než jak je upraveno těmito podmínkami nebo než jak vyplývá z platných právních předpisů.

1.5. Okamžikem Nabytí se pro účely použití Licence produktu ELDAx rozumí datum zdanitelného plnění uvedené na daňovém dokladu vystaveného dodavatelským subjektem. V případě neexistence takového dokladu, může tento dokument nahradit jiný doklad, jednoznačně určující datum pořízení licence ELDAx Nabyvatelem.

1.6. Součástí Daňového dokladu, nebo jeho příloh, musí být zřejmá konfigurace licence, tj. seznam komponent a modulů, ke kterým Nabyvatel získal právo užití dle této licenční smlouvy.

Majitel autorských práv

1.7. Majitelem všech autorských práv k produktu ELDAx SMART TRUST ELECTRONIC PLATFORM je společnost TECHNISERV IT, spol. s r.o., Traťová 1, BRNO, ČESKÁ REPUBLIKA, IČ 26298953, spisová značka: C 42557 vedená u Krajského soudu v Brně.

2. Typy licencí SW produktu ELDAx

2.1. Licence typu UnLimited obsahuje tyto práva užití ELDAx:

2.1.1. Přístup z klientských zařízení: ELDAx může být na zařízení prostřednictvím klientské aplikace používán k běžnému užití – tj. může být spouštěn, mohou být prohlížena, vkládána nebo v něm měněna data pomocí klientské aplikace, či je možné data jiným způsobem užívat na neomezeném počtu zařízení používaných zaměstnanci Nabyvatele. Toto ustanovení se vztahuje na všechna Zařízení, která technologicky umožňují přístup z klientských zařízení. Zařízením se rozumí server, počítač, pracovní stanice, terminál, PDA, zařízení typu „inteligentní telefon" nebo jiné elektronické digitální zařízení, na kterém jde pomocí klienta přistupovat k ELDAx. Zařízení jako takové nemusí být ve vlastnictví Nabyvatele, ale osoba používající toto zařízení musí být zaměstnancem Nabyvatele, pokud nesplňuje některou z podmínek níže.

2.1.2. Přístup ze serverových aplikací Nabyvatele prostřednictvím integračního rozhraní: Do ELDAx může vstupovat jakákoliv aplikace, systém informačního systému Nabyvatele. Prostřednictvím standardního integračního rozhraní (SInRo) aplikace mohou využívat jakékoliv služby ELDAx dostupné na tomto Standardním Integračním Rozhraní (tj. mohou být vkládány, nebo čteny dokumenty, měněna popisná data a další informace, konzumovány služby důvěryhodnosti, prováděna administrace). Aplikace musí být v majetku Nabyvatele, nebo je musí mít pro své potřeby pronajaté.

2.1.3. Využití rozhraní SInRo je pro aplikace třetích stran možné výhradně v případech, kdy je účelem předávání strukturovaných dat, která jsou v okamžiku zapsání do ELDAx v majetku a správě Nabyvatele, a nejedená se o způsob využití mající podobu a charakter pro který je určená licence Datacenter.

2.1.4. Produkční serverová licence (Proserver) opravňuje instalovat a používat jednu instanci ELDAx pro produkční provoz Nabyvatele. Licence neopravňuje k instalaci ELDAx současně na více Zařízeních nebo provozu ve více instancích.

2.1.5. Testovací serverová licence (Testserver) opravňuje Nabyvatele instalovat jednu instanci ELDAx do testovacího prostředí Nabyvatele a může být použita výhradně pro „Testovací Provoz". "Testovací provoz" je realizován nad testovacími daty, tedy neúplnými daty z pohledu komplexity, určenými k realizaci testovacích scénářů, a má za cíl prověřit funkcionality ELDAx nebo souvisejících aplikací. V rámci testovacího provozu může Nabyvatel prověřovat zejména soulad uživatelských vlastností ELDAx nebo integrovaných Systémů – aplikací. Výstupy jakýchkoliv testovacích činností nesmějí být použity pro jiné účely, než optimalizace nastavení ELDAx nebo integrovaných aplikací s ELDAx.

2.1.6. Školící a serverová licence (Eduserver) opravňuje instalovat jednu instanci ELDAx do školícího prostředí Nabyvatele. Nabyvatel ve školícím prostředí

zvyšuje úroveň ovládání a poznání ELDAx pro uživatele nebo administrátory. Výstupy jakýchkoliv školících činností a instalace Eduserver nesmějí být použity pro jiné účely, než zvyšování znalosti uživatelů nebo administrátorů ELDAx .

2.2. Moduly serverové licence Proserver, Testserver, Eduserver: Moduly nebo komponenty ELDAx se rozumí moduly řešení ELDAx. Tyto se pořizují volitelně, společně se základní licencí produktu ELDAx. Pořízené Moduly či komponenty mohou být používány pouze současně s Produkční, Testovací nebo Školící serverovou licencí. Pokud není u modulu výslovně stanoveno jinak, používá se v souladu s těmito licenčními podmínkami. Seznam pořízených modulů je součástí nabývacího dokumentu a je označován jako konfigurace licence ELDAx.

2.3. Afilace licence. Opravňuje k užití ELDAx zaměstnanci jedné jiné fyzické či právnické osoby, která je ve vztahu afilace k vlastníkovi licence. Afilační licence neopravňuje k instalaci další instance ELDAx. Afilací ve smyslu těchto Licenčních podmínek se rozumí vztah mezi oprávněným z licence a kteroukoliv právnickou osobou, kterou vlastní, která vlastní jeho nebo je s ním společně vlastněna. Vlastnictví pro účely této definice znamená větší než **50%** přímý nebo přepočtený majetkový podíl na právnické osobě.

3. Omezení některých Typů licencí ELDAx

3.1. AppLimited Licence. Opravňuje k užití ELDAx pouze pro ruční vkládání, čtení nebo jiné zpracování dat prostřednictvím uživatelského webového rozhraní a využití ELDAx způsobem, jak je popsáno v odstavci v licenci UnLimited, je omezeno pouze na jednu aplikaci přistupující kontinuálně v průběhu 12 měsíců. Jakékoliv další aplikace nemají do ELDAx prostřednictvím Standardního Integračního Rozhraní (SInRO) přístup.

3.2. Lite Licence: Opravňuje k užití ELDAx pouze pro ruční vkládání, čtení nebo jiné zpracování dat prostřednictvím uživatelského webového rozhraní a je možné ji využít výhradně pro komponentu ELDAxSTORAGE.

3.3. Time Limited Licence. Časově omezená licence Opravňuje k užití ELDAx v souladu s těmito Licenčními podmínkami. Udělená licence je časově omezena. Doba, na kterou je licence omezena je uvedena v označení licence v nabývacím dokumentu za označením „TIME LIMITED:“

3.4. Trial Licence: Softwarové produkty označené jako ELDAx TRIAL může Nabyvatel získat bezúplatně a může je užívat na libovolném počtu Zařízení současně. K tomuto typu licence se neváží žádné záruky, ani odpovědnost za vady či škodu. Tyto licence nesmějí být použity pro komerční účely, jsou určeny výhradně k prověření deklarovaných funkcí produktu ELDAx.

3.5. Žádná licence ELDAx, vyjma edice ELDAx Datacenter není určena k pronájmu

nebo sdílení, poskytování sublicencí jiným subjektům (právnické nebo fyzické osobě), nebo k využitím třetím osobám s výjimkou případů, kdy třetí osoba zajišťuje provozní potřeby Nabyvatele nebo splňuje podmínky afilace a její přístup je pokryt udělenou Afilační licencí.

4. Operace s licencemi ELDAx

4.1. Patch management ELDAx a přechod na nové verze: V rámci licence má Nabyvatel právo na přístup k aktualizacím, upgrade, update ELDAx, komponent nebo jeho Modulů. Toto ustanovení platí výhradně v případě, že má Nabyvatel řádně pořízené maintenance produktu ELDAx.

4.2. Změna Typu licence: Změna typu licence znamená změna na úrovni AppLimited, UnLimited, Time Limited nebo jiného typu licence.

4.3. Rozšíření licence: jedná se o doplnění daného Typu a konfigurace licence o další modul nebo komponentu.

4.4. Převod Licence: Veškerá práva a povinnosti vyplývající z těchto Licenčních podmínek může Nabyvatel postoupit na nový subjekt pouze po předchozím písemném souhlasu registrovaného partnera, oprávněného dodávat licence ELDAx, nebo výrobce ELDAx. Seznam partnerů je dostupný na www.eldax.cz. V případě udělení souhlasu pro převod licence musí Nabyvatel převést na Nový Subjekt veškeré licence ELDAx a jejich součásti (včetně všech rozšiřujících licencí, komponent, médií, tištěného materiálu a aktuální verze Smlouvy) a ze svých Zařízení zcela odstranit všechny instance ELDAx nebo jeho Modulů. Předpokladem možnosti převodu je i písemný souhlas Nového Subjektu s realizací převodu a s těmito Licenčními podmínkami.

5. Ochranné známky ELDAx

5.1. Tyto Licenční podmínky neudělují Nabyvateli žádná práva ve spojení s ochrannými známkami ELDAx.

5.2. REVERZNÍ INŽENÝRSTVÍ ZA CÍLEM ANALÝZY ELDAx, JEHO MODULŮ NEBO KOMPONENT: Nabyvatel nesmí jakkoli využít znalosti o myšlenkách, postupech, struktuře, algoritmu a použitých metodách, na nichž je ELDAx založen nebo které obsahuje, i když je získal při oprávněném užití ELDAx, vyjma jejich nezbytného užití k dosažení vzájemného funkčního propojení ELDAx s jinými počítačovými programy pomocí standardního integračního rozhraní ELDAx. Tyto znalosti nesmí být využity ani k vývoji, zhotovení nebo k obchodnímu využití jiného počítačového programu, ani k jinému jednání ohrožujícímu nebo porušujícímu autorské právo ELDAx.

5.3. O znalostech získaných při integračních činnostech je Nabyvatel povinen zachovávat mlčenlivost vůči třetím osobám.

5.4. Licence ELDAx, komponent a modulů se uděluje výhradně na produkt v

kompilovaném tvaru.

6. Ukončení licence, práva k užití ELDAx

6.1. V případě porušení tohoto Licenčního ujednání Nabyvatelem nebo vypršení časového omezení u TIME LIMITED licence zaniká Nabyvateli právo na užívání licence.

6.2. Tímto ustanovením nezaniká povinnost nabyvatele uhradit vlastníkovi autorských práv k ELDAx za neoprávněně užité licence a zároveň nezaniká náhrada na úhradu vzniklé škody.

6.3. V případě ukončení práva užití ELDAx na základě těchto Licenčních podmínek končí veškerá práva užití ELDAx vč. jeho Modulů a komponent poskytnutá Nabyvateli.

6.4. V takovém případě musí Nabyvatel nejpozději v den ukončení práva užití ELDAx ze všech svých počítačů zcela odstranit všechny instalace ELDAx a jeho modulů a komponent.

7. Závěrečná ustanovení

7.1. Tyto licenční podmínky jsou platné od 1. 1. 2023 a nahrazují předchozí „LICENČNÍ PODMÍNKY SOFTWAROVÉHO ŘEŠENÍ ELDAx“.

7.2. Licenční podmínky jsou účinné pro všechny nové licence ELDAx pořízené po jejich datu platnosti.

7.3. Licenční podmínky jsou účinné pro všechny licence ELDAx, u kterých došlo po datu jejich platnosti k jakékoliv „operaci“ s licencí v souladu s článkem 4.

7.4. Pokud soud rozhodne, že některé z ustanovení těchto Licenčních podmínek jsou neplatné, zůstávají zbývající ustanovení platná a účinná.

Standard systémové bezpečnosti

Označení: SSB
Verze: 1.1

Platnost od: 20. 9. 2021

	Údaje o vydání		
	Zpracoval:	**Odpovědný pracovník:**	
Funkce:	Business analytik	vedoucí oddělení správy a rozvoje IS	
Jméno:	[redacted]	[redacted]	
Datum:	*19.9.2021*	*25.9.2021*	

Obsah:

1. Úvodní ustanovení

1.1. Účel standardu

Účelem standardu je definovat základní rámec pro implementaci bezpečnosti aplikací a systémů zaváděných nebo provozovaných v infrastruktuře LČR.
Tento rámec je tvořen vymezením bezpečnostních požadavků, které musí splňovat aplikace a systémy vyvíjené, dodávané a rozvíjené v prostředí LČR. Jedná se o definované procesy, postupy, opatření a jejich naplnění vzhledem k požadované úrovni zabezpečení.
Cílem naplnění standardu systémové bezpečnosti je sjednotit požadavky na povýšení bezpečnosti u všech dodávaných, vyvíjených nebo rozvíjených systémů. Předmětem standardu jsou tedy rozvíjené nebo vyvíjené a dodávané aplikace, informační systémy na míru nebo podobné programy a řešení, a dále i komerční software, které jsou dodávány za účelem poskytování agendy a její podpory vymezené zákonem nebo poskytování informačních služeb pro interní potřeby v prostředí LČR (dále jen „Systém“).

1.2. Rozsah působnosti

Standard je závazný pro všechny zaměstnance LČR, a to jak ve služebním, popřípadě pracovním poměru, tak i zaměstnaných na základě dohod o pracích konaných mimo služební, popřípadě pracovní poměr (dále jen „zaměstnanci“), a dále pro všechny osoby a externí strany vykonávající práce pro LČR na základě smluvního vztahu či občanského zákoníku (dále jen „externisté“), kteří spolupůsobí při rozvoji, vývoji nebo zavádění Systému.

1.3. Pojmy a zkratky

Pojmy a zkratky používané v tomto standardu jsou uvedeny v tabulce na konci tohoto dokumentu.

2. Rozdělení a definice požadavků na zabezpečení

Požadavky na zabezpečení Systému jsou v tomto dokumentu rozděleny na čtyři základní oblasti, vztahující se k jednotlivým atributům bezpečnosti, tak jak jsou chápány obecně i směrem k bezpečnosti Systému. Jedná se o tyto oblasti:

2.1. Důvěrnost

Musí být zajištěna mechanismy se schopností ujistit se, že je vynucena nezbytná úroveň míry utajení v každém okamžiku, kdy dochází ke zpracování dat a je zajištěna prevence jejich neautorizovaného vyzrazení. Taková úroveň důvěrnosti musí přetrvat minimálně během uchovávání dat v Systému a při jejich přenosu k adresátovi. Rozpracováno v kap. 3.1.

2.2. Integrita

Musí být zajištěna identifikací přesnosti, zaručeného obsahu a musí být provedena opatření proti jejich neautorizované změně. Hardwarové, softwarové a komunikační prostředky musí pracovat tak, aby data uchovávaly a zpracovávaly správně a přesně, přenášely je do požadovaného cíle bez nežádoucích změn. Celkově musí být Systém a síť chráněny před vnějším rušením či kontaminací původní informace. Rozpracováno v kap. 3.2.

2.3. Dostupnost

Musí být zajištěna spolehlivou a včasnou dispozicí dat a zdrojů autorizovaným jednotlivcům. Systém a sítě musí mít datovou kapacitu dimenzovanou tak, aby v definovaném čase poskytovaly dostatečný

výkon, a musí být schopny zotavit se z výpadků transparentním a rychlým způsobem. Proto musí být zavedeny redundantní mechanismy a navrženy záložní řešení pro možnost rychlé náhrady. Součástí proškolení uživatelů k Systému musí být postup nebo návod jak provést jeho uvedení do funkčního stavu. Pokud jsou opatření realizována na infrastrukturní vrstvě, nebudou požadována. Rozpracováno v kap. 3.3.

2.4. Metodika vývoje a ostatní požadavky

Představuje zavedení souhrnu postupů, pravidel a nástrojů používaných pro návrh, plánování a řízení vývoje software. Metodikou se též rozumí využití těchto položek nebo dalších specifických postupů pracovním týmem nebo celou organizací při vývoji aplikačního software nebo informačního.

3. Požadavky na Systém

3.1. DŮVĚRNOST

3.1.1. Řízení přístupu

Systém musí zajišťovat tvz. AAA (Autentizaci, Autorizaci, Audit) v potřebné úrovni dle jeho konkrétní specifikace.

- Systémy, které obsahují citlivá data, musí podporovat vícefaktorovou autentizaci.
- Systémy typu webové aplikace musí umožňovat autentizaci zašifrovaným kanálem (pomocí TLS), tak, aby přihlašovací údaje neprocházely síťovou infrastrukturou v otevřeném tvaru.
  Musí existovat možnost oddělení rolí v Systému, minimálně pro:
  - administrátory,
  - uživatele,
  - auditory.
- Správa interních a externích uživatelských entit musí být oddělena.
- Musí existovat možnost šifrování přenosu i uložení citlivých uživatelských dat.

Registrace, autentizace a identifikace uživatelů.

Systém musí umožňovat:

- registraci všech uživatelů centrálně,
- stanovit pravidla pro procesy:
  - registrace,
  - schvalování,
  - generování identit,
  - přidělování a odebírání přístupů,
  - deaktivace identit,
  - monitorování činnosti uživatelů.

Tyto funkce musí být v Systému buď přímo implementovány, nebo může Systém využívat stávajících podsystémů pro podporu identifikace a autentizace v prostředí LČR.

Pokud v rámci Systému nebo jeho komponent a podpůrných podsystémů existují lokální účty, musí se řídit následující politikou hesel pro privilegované účty nebo musí umožnit integraci se systémem pro správu privilegovaných účtů.

Řízení hesel je vázáno na aktuální bezpečnostní politiku platnou v době implementace řešení a v závislosti na její definici se parametry politiky pro vytváření hesel mohou měnit. Dodavatel Systému se při tom musí řídit aktuálním zněním směrnice OICT LČR.

Týká se požadavku na vznik nebo změny rolí, v požadavku musí být popsáno včetně rozsahu oprávnění. Za dodržení principu „least privilege“ (minimálních oprávnění) je odpovědná aplikační definice. Vztahuje se k textu v kap. 3.1.1, především k oddělení rolí, monitorování činnosti uživatelů, lokálním účtům.

3.1.2. Autorizace

Autorizace uživatelů musí probíhat na základě stanovených uživatelských rolí. Pro ověření uživatelů v Systému musí být přímo v něm implementována funkce ověření uživatelů nebo musí využívat stávajících systémů pro podporu autorizace v prostředí LČR. Současné ověřování uživatelů je řízeno adresářovou službou (LDAP) resp. jejich členstvím ve skupinách (tedy LDAP skupina = role v Systému). Systém musí mít vyhrazenu větev LDAP adresáře, ve kterém existují vlastní skupiny. Systém se pomocí protokolu LDAP připojí do LDAP adresáře, ze kterého následně vyčítá informace o členství ve skupinách, na základě kterých se dále rozhoduje o autorizaci (oprávnění). Pokud bude nutné z důvodu komplexnosti a složité údržby (např. oprávnění přístupu k jednotlivým objektům) udržovat některá oprávnění pouze lokálně, musí být udělena výjimka manažerem kybernetické bezpečnosti. Systém musí navíc v takovém případě poskytovat vhodné rozhraní pro jejich export, včetně vazeb na uživatele (webová služba, JDBC, soubor).
Pro Systém musí být definovány samostatné uživatelské role, které se dále člení dle aplikačních požadavků.

3.1.3. Infrastrukturní privilegované účty

Na všech podpůrných systémech a komponentách (OS, DB, atp.) musí být zavedeny privilegované účty, výhradně personifikované, které představují přidělení samostatných přihlašovacích údajů pro jednotlivé administrátory. Použití sdílených administrátorských účtů musí být řádně odůvodněno a schváleno výjimkou manažera kybernetické bezpečnosti LČR.

Týká se požadavků, jejichž předmětem je infrastrukturní typ účtů včetně servisních nebo technických účtů viz také kap. 3.1.4 a 3.1.6

3.1.4. Servisní účty

Servisní nebo také technické účty, pod kterými běží Systém či jeho jednotlivé komponenty, pod kterými jsou jakýmkoli způsobem impersonifikována vlákna, systémová či meziprocesová volání, nebo prostřednictvím kterých Systém přistupuje k ostatním komponentám nebo externím systémům, musí být uvedeny v dokumentaci k Systému. U každého účtu musí být uveden jeho účel a způsob jakým je možné účtu změnit heslo, včetně identifikace všech míst, kde je takové heslo uloženo (DB tabulka, konfigurační soubor v zašifrované podobě, atp.). Hesla k servisním účtům musí být předána LČR bezpečným způsobem dle smluvně stanovených podmínek.

Týká se požadavků, jejichž předmětem je infrastrukturní typ účtů včetně servisních nebo technických účtů.

3.1.5. Omezení oprávnění

Pro všechny typy účtů (uživatelské, administrátorské, servisní) je vždy uplatněn “princip minimálních oprávnění“ (principle of least privilege), tedy že každý účet má nastavena pouze taková oprávnění, která jsou nezbytná pro provádění činností, ke kterým byl účet zřízen. Princip minimálních oprávnění se vztahuje též na oprávnění ke stránkám v režimu chráněné paměti.

Pro servisní účty se dále uplatňuje "princip oddělení privilegií" (principle of privilege separation), na základě kterého má každá komponenta (funkční část) pouze taková oprávnění, která potřebuje pro svoji funkci a tedy využívá svůj vyhrazený servisní účet s příslušnými oprávněními.

3.1.6. Procesní řízení účtů

Proces **přidělování/odebíraní oprávnění** a **vytváření/rušení účtů** v Systému a podpůrných komponentách (OS, DB, atp.) je zřizován přes Helpdesk systém LČR.

Týká se požadavků, jejichž předmětem je infrastrukturní typ účtů včetně servisních nebo technických účtů.

3.1.7. Auditní mechanismy Systému.

S ohledem na požadavek zajištění auditovatelnosti dat i procesů v Systému je nezbytně nutné zabudovat tuto možnost při návrhu a vývoji Systému. Jedná se zejména o přístupy i změny v datech pro jednotlivé objekty. Rovněž proces řízení identit uživatelů musí být auditovatelný.

Auditní mechanismy by měly být zavedeny na 2 úrovních:

1. **Dohledatelnost provedených změn v datech příslušné agendy**
2. **Centrální logování událostí v systému**

Ad 1) Dohledatelnost provedených změn v datech příslušné agendy

Na úrovni fyzických tabulek s uloženými daty příslušné věcné agendy je minimálně nutné zajistit

- Auditní sloupce Kdo (jaký login) a Kdy záznam vytvořil
- Auditní sloupce Kdo a Kdy daný záznam naposledy změnil
- Tato auditní stopa musí být zajištěna i v případě přímých operací v databázi

Výše uvedené sloupce nemusí být řešeny na úrovni každé tabulky s daty pro příslušnou agendu, jestliže systém disponuje jiným mechanismem pro logování změn, který zajistí snadnou publikaci auditních dat na uživatelské rozhraní.

Jestliže v rámci požadavku bude výslovně požadována plná historizace dat příslušné agendy, je systém povinen na úrovni databáze zajistit takovou formu historizace, která umožní historizovaná data včetně časových otisků změn prezentovat v případě změn jednoduše na uživatelském rozhraní, a to atomizovaně po každé dílčí změnové události. (standardním řešením je opatření tabulky systémovými sloupci Od-Do , event. sloupcem Smazáno a sloupci, které nesou informaci o autorovi změny).

Ad 2) Centrální logování událostí v systému

Logy Systému musí být integrovány do aktuálního centrálního řešení pro správu a vyhodnocování logů, které je provozováno v prostředí LČR. Systém tedy musí umožnit takovou integraci. Logy Systému musí být dostupné bez prodlení od vzniku události, a integrovány do centrálního logovacího nástroje v jím podporovaných formátech minimálně jednou z následujících metod:

- Syslog
- SNMP TRAP
- Textový soubor
- JDBC
- Microsoft Event Log

Dodavatel Systému zajistí definici rozsahu Systému vzhledem k infrastruktuře a tedy, které části infrastruktury a podpůrné komponenty jsou jeho součástí a doporučí vzhledem k bezpečnostním

dopadům jejich bezpečnostní monitoring. Dodavatel zajistí přístup k auditním logům a doporučí způsob jejich vyčítání v souladu s těmito standardy.

V rámci LČR musí být pořizovány a uchovávány auditní záznamy zejména takové, které jsou uvedeny ve výčtu níže, tak, aby byly využitelné pro monitorování řízení přístupu a případné budoucí vyšetřování bezpečnostních incidentů. Zaznamenávání událostí zohledňuje technické možnosti Systému a pro sběr záznamů ukládá minimálně tyto typy událostí:

- přihlášení a odhlášení uživatelů a administrátorů,
- činnosti provedené administrátory,
  - použití privilegovaných účtů, např. účtu supervisora, administrátora,
  - spuštění a ukončení Systému,
  - změny konfigurací,
- činnosti vedoucí ke změně přístupových oprávnění,
- neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti uživatelů,
- zahájení a ukončení činností technických aktiv,
- automatická varovná nebo chybová hlášení technických aktiv,
- přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností,
- použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení.

Jednotlivé položky logu Systému nebo jeho jednotlivé řádky záznamu musí obsahovat minimálně tyto pole:

- ID záznamu
- Datum a čas události (uvedený s jednoznačnou identifikací časové zóny, např UTC nebo lokální čas s uvedením offsetu)
- síťové identifikátory komunikujících bodů (tj. např. IP adresy a porty)
- Uživatelský identifikátor
- ID Typu události
- Popis události
- Detail události

Textová pole musí být oddělena pomocí znaku„|“ (pipe, ASCII kód 124) a musí být vytvořen číselník ID typu událostí dle typických událostí v Systému a předán v dokumentaci.

Pokud údaje zapisované do logu Systému obsahují citlivá data (heslo, klíč či jeho prekurzor, session ID apod.) nesmí být uložena v plain textu, ale musí být před zapsáním zašifrovány nebo přepsány pseudonáhodnou sekvencí;

V Systému musí být zavedena ochrana proti deaktivaci, selhání či změnám v pořizování auditních záznamů a ochrana proti změnám nebo zničení auditních záznamů.
Přístup k auditním záznamům musí být bezpečně chráněn, aby bylo zabráněno jeho zneužití nebo ohrožení. Systém musí umožnit nastavení přístupových práv k auditním záznamům tak, aby mohly být auditovány samostatnou rolí (auditor, security officer a.p.).

Konkrétní požadavky mohou brát zřetel na potřebu historizace záznamů (stav záznamů k určitému datu), musí zde ale existovat oprávněná potřeba vzhledem ke kapacitní náročnosti jejího zajištění. Zadavatel a dodavatel zvažuje, zda existují legislativní nebo věcné požadavky na možnost historizace dat.

3.1.8.Šifrování

Veškerá citlivá data musí být adekvátním způsobem zabezpečena kryptografickými metodami, které zajistí pouze autorizovaný přístup. Ochrana dat musí být zaručena během celého jejich životního cyklu, tedy jak při jejich přenosu tak jejich uchovávání. V rámci kryptografických metod musí být Systém připraven na využívání kryptografických algoritmů, které jsou v souladu s Přílohou č. 3 k vyhlášce č. 316/2014 Sb., (vyhláška o kybernetické bezpečnosti).

Závazné detaily nastavení šifrování k jednotlivým protokolům jsou definovány ve zde vloženém dokumentu, a to vždy v jeho aktuální verzi:

Týká se požadavků realizujících kryptografickou ochranu na úrovni aplikace. Týká se i kap. 3.1.9

technické_požadavky.xlsx

3.1.9.Certifikační autority

Systém musí být připraven využívat při autentizaci uživatele a ověřování digitálního podpisu kvalifikované certifikační autority v ČR a ze zemí EU, interní CA LČR, případně jinou CA nastavenou jako důvěryhodnou.

Systém musí umožnit elektronické podepisování a schvalování dokumentů prostřednictvím zapojení do procesů interního PKI pro správu uživatelských klíčů nebo pro vytváření elektronických značek a pro autoritu časových razítek, pokud Systém tyto procesy využívá. Ve všech těchto případech se Systém též musí řídit certifikační politikou a prováděcími směrnicemi zúčastněných CA.

Při ověřování certifikátu, ať už jde o certifikát protistrany v komunikaci nebo certifikát pro ověření elektronického podpisu či časového razítka, musí Systém implementovat algoritmus ověření certifikátu minimálně s těmito kontrolami:

- sestavení certifikační cesty až k důvěryhodnému certifikátu
    - lze použít atribut AIA k dotažení certifikátů mezilehlých CA
    - musí být možnost použít statickou cache certifikátů mezilehlých CA
    - preferovaně používat certifikáty mezilehlých CA, které jsou součástí TLS handshake či obálky elektronického podpisu
    - neúspěšné sestavení jedné certifikační cesty není samo o sobě důvodem pro ukončení ověřování certifikátu s negativním výsledkem, pokud lze sestavit alternativní certifikační cesty (např. v prostředí s křížovou certifikací kořenových CA)
- pro všechny certifikáty v certifikační cestě, které nejsou explicitně důvěryhodné, je nutno ověřit:
    - uvedení daného certifikátu podle jeho hashe či hashe veřejné části jeho klíče na seznamu explicitně nedůvěryhodných certifikátů
    - platnost certifikátu vzhledem k
        - aktuálnímu času
        - nebo k času podpisu, pokud je tato hodnota v ověřitelné časové značce svázané s ověřovanými daty (kontrasignace TSA)

    - atributy Basic Constraints (Entity Type, Path Length Constraint), Name Constraints, Key Usage a Extended Key Usage, jsou-li v certifikátu uvedené, pro dané použití certifikátu a klíče, a to bez ohledu na jejich kritičnost
    - sílu podpisového algoritmu, popř. i ve vztahu k době platnosti a/nebo aktuálnímu času, pokud je použití daného algoritmu či velikosti klíče časově omezeno
    - platnost digitálního podpisu veřejnou částí klíče nadřízené CA
    - OID certifikační politiky, pokud je pro dané použití omezena
    - zneplatnění certifikátu před koncem doby platnosti podle:
        - CRL
            - lze použít atribut CRL DP pro dotažení aktuálního CRL
            - musí být možnost použít statickou cache s CRL
        - OCSP
            - online komunikací s OCSP responderem podle URL v atributu AIA
            - OSCP stapling, pokud jej daný protokol (např. TLS) podporuje
    - v případě, že certifikát obsahuje atribut (atributy), označený (označené) jako kritické, které ověřovací algoritmus buď nezná, nebo nemůže jejich kontrolu z nějakého důvodu provést (např. kvůli chybě v komunikaci), musí být ověřování certifikátu ukončeno jako neúspěšné
    - pokud ověřování v certifikační cestě není úspěšné
        - je možné použít alternativní certifikační cesty, pokud je lze sestavit (např. v prostředí s křížovou certifikací kořenových CA)
        - v případě, že se selhání váže k obsahu či stavu platnosti koncového certifikátu, alternativní cesty se již nepoužijí
- pokud se ověření certifikátu váže na identitu protistrany (hostname v URL, IP adresa vzdáleného konce IPSec apod.) či původce (např. E-mailová adresa odesilatele podepsané zprávy), pak pro porovnání:
    - pokud není přítomen atribut Subject Alternative Name (SAN), použije se atribut Subject
    - pokud je přítomen atribut SAN, použije se preferovaně ten; volitelně, pokud se nenalezne shoda v atributu SAN, může se použít i atribut Subject

Týká se požadavků realizujících kryptografickou ochranu na úrovni aplikace.

3.2. INTEGRITA

Cílem je zaručení a udržení konzistence a správnosti dat během jejich celého životního cyklu. Je tedy potřeba zajistit, aby data nemohla být neautorizovaně modifikována a aby každá autorizovaná i neautorizována modifikace dat byla detekována a zaznamenána. Spolu s integritou je žádoucí zajistit také nepopiratelnost, tedy vyloučení možnosti popřít provedení libovolné operace nad daty. V základu je integrita dat zajištěna pomocí vhodného řízení přístupu k datům (autorizace) a auditovatelnosti (logování a následná detekce přístupu k datům). Integrita kritických dat musí být zajištěna implementací kontrol – např. počítání kontrolních otisků dat a jejich pravidelná kontrola, dále též kryptografické zajištění kontrolních otisků dat (elektronický podpis, HMAC, hash tree).
Každý vstup do Systému (externí systém, uživatel, mezi komponentami) je vždy kontrolován na typovou a logickou správnost, čímž může být detekováno poškození dat, nebo případný pokus o útok. V definovaných případech se provádí validace dat dle specifikace v zadávací dokumentaci, ta určuje základní parametry a určuje kvalitu vstupů se zaměřením např. na kontrolu správného formátu dat, kontrolu mezí, přítomnost povinných dat, logických závislostí mezi daty apod. Architektura řešení bere v úvahu bezpečnostní aspekty prostředí. Systém musí být navržen mimo jiné tak, aby respektoval jednotlivé bezpečnostní přiřazení komponent Systému k zónám důvěryhodnosti a jejich rozmístění do jednotlivých bezpečnostních zón prostředí.

Standardními opatřeními pro zajištění integrity kromě zajištění dohledatelnosti změn je

1. **používání databázových nástrojů primárně na úrovni transakčních dat**
   - Používání cizích klíčů při vazbě na číselníkové hodnoty anebo nadřízené entity
   - Používání constraints zamezujících vložení prázdné hodnoty do sloupců, kde v žádném případě se neočekává prázdná hodnota
   - Používání unikátních klíčů nad sloupci, které z povahy věci musí obsahovat unikátní záznamy
2. **používání aplikační logiky kontrolující platnost dat**
   - Platnost podřízené entity by neměla přesahovat platnost nadřízené entity
   - PlatnostDo by nikdy neměla předcházet PlatnostiOd
3. **používání kontrol na data vstupujících do systému**
   - Vstupní formuláře musí používat elementární kontroly na správnost formátu datumu, čísla, a plnění povinných hodnot apod.
   - Jestliže určité pole má definovanou délku a formát, pak musí být na vstupním formuláři prováděna adekvátní kontrola

V případě, že se systém má od těchto pravidel odchýlit, pak v příslušném požadavku tato odchylka bude popsána.

3.3. DOSTUPNOST

Dostupnost Systému musí být stanovena a definována na požadovanou úroveň. Podle této definice se dále stanoví architektura celého řešení s ohledem na dostupnost, ve smyslu redundantních a clusterovaných schémat v režimu vysoké dostupnosti (HA), stanovení úrovně podpory, DRP a zálohování.

Týká se požadavků realizujících opatření v kap.3.3 na úrovni aplikace.

3.3.1. Řešení vysoké dostupnosti (HA)

Dodavatel Systému navrhne v rámci architektury řešení, způsob zajištění vysoké dostupnosti Systému dle jeho definice úrovně dostupnosti. Ta musí být zajištěna pomocí redundantních nebo clusterovaných schémat přímo v návrhu architektury.

Postupy obnovy po havárii - Disaster recovery planning
Dodavatel Systému navrhne postupy pro vypnutí a zapnutí Systému, včetně posloupnosti jednotlivých kroků, především s ohledem na bezpečné obnovení Systému při jeho selhání – tj. vytvoření plánů obnovy aplikace. Dále je povinen spolupracovat na jeho ověření v rámci testování obecných plánů obnovy provozu Systému LČR, uvedené též v části Testování.

3.3.2. SPOF

Při návrhu HW platformy, logické a fyzické komunikace a datových toků obecně, musí být zohledněno dodržování pravidla eliminace „SPOF“ (Single Point of Failure) – tedy, že porucha jedné komponenty nezpůsobí výpadek celého Systému. Jedná se o serverovou infrastrukturu, datové úložiště, zálohování a další prvky celé LAN.

Server	Co zálohovat	Jak často full backup	Kolik k záloh držet	Kolik dní držet zálohy	Jak často inkrement backup	Kdy probíhá záloha	Předpoklá daná doba obnovy
Server-x	Celý server	1*týdně	30		denně	18:00-18:10	30 minut
Server-x	Databáze A	2*denně	28			8:00-8:10, 20:00-20:10	10 minut

Server-x	Databáze A – transakční logy			730	Každou transakci	Dle transakcí	10 minut
Aktivní prvek-X	Konfigurační soubory	Při každé změně	10			Dle změn	30 minut

3.3.3. Zálohování

Návrh Systému musí obsahovat požadavky na zálohování, které vychází ze SLA parametrů aplikace. Vždy se požaduje vytvoření detailního návrhu zálohování celého Systému včetně návaznosti na stávající zálohovací systém LČR. Popis by měl mít strukturu, viz vzor níže

3.4. METODOLOGIE PRO VÝVOJ A OSTATNÍ POŽADAVKY

Dodavatel musí mít formalizovanou Metodologii pro vývoj, programování a kódování aplikace zahrnující i požadavky na bezpečnost, včetně opatření na ochranu proti škodlivým programům nebo postupům. Metodologie musí též zahrnovat základní principy organizační bezpečnosti pro vývoj a testování aplikace. Dodavatelé musí doložit typ metodologie, který použil pro vývoj aplikace prostřednictvím čestného prohlášení a dodání popisu nebo dokumentace této metodologie.

3.4.1. Data

Systém musí poskytovat podporu pro správu klasifikovaných dat.

Dále pak je požadováno, aby řešil vstupně - výstupní validaci dat tak, aby odesílaná a přijímaná data byla kontrolována na typovou a logickou správnost při jejich zadávání nebo exportu.
Šifrování ukládaných dat musí být prováděno s ohledem na požadavky zajištění důvěrnosti dat, kde je vždy nutné využít vhodného šifrování ukládaných dat, které zajistí tento požadavek na důvěrnost viz kapitola 3.1.8

Viz kapitola 3.2.

3.4.2. Lokalizace

Systém musí podporovat českou národní lokalizaci a přednostně vícebajtové kódování (UTF8 s povinností uvádět BOM).

3.4.3. Výjimky běhu, chyby a hlášení

Systém musí podporovat řízení výjimek, kdy výjimkou se myslí libovolná chyba nebo neočekávané chování, které se vyskytne během vykonávání programu a je následně zpracováno a zároveň nedojde k neřízenému selhání běhu.
Standardem je, že při vzniku chyby běhu programu bude zobrazeno dialogové okno s identifikátorem chyby mající vazbu na log události aplikace, pod kterým je situace následně v lozích dohledatelná, přičemž musí existovat oddělení uživatelských hlášení od technických. Uživatelská hlášení nesmí obsahovat technické detaily, které by bylo možné použít k další exploitaci, ale jen index, který odkazuje na jeho popis mimo systém. Opakované a známé chyby je vhodné opatřit kódem a smysluplným popisem. Uživatelská hlášení musí být uvedena v českém jazyce.

3.4.4. Práce s pamětí

Kód Systému musí implementovat vhodná opatření při práci s pamětí:

- již nepoužívané objekty a jiné datové struktury jsou z paměti odstraňovány;
- pokud datová struktura obsahuje citlivá data (heslo, klíč či jeho prekurzor, session ID apod.), musí být před dealokací tyto hodnoty přepsány pseudonáhodnou sekvencí;
- je nutné zajistit, aby datovou strukturu, označenou k dealokaci, nebylo možné dereferencovat (tj. odstranit před dealokací všechny ukazatele na dealokovanou strukturu);
- paměťové stránky, které obsahují pouze data, nebyly zároveň označeny jako stránky se spustitelným kódem;
- nepřímé skoky (např. volání virtuální metody) musí před vlastním provedením volání zkontrolovat, zdali je adresa volaného kódu legitimní.

3.4.5. Řízení konfigurace a změn

Systém musí mít zavedeno řízení konfigurace a změn, které představuje systematické vyhodnocování, koordinování a implementaci schválených změn, včetně uchování předchozích verzí a testování verzí nových.

3.4.6. Bezpečnost, provoz a správa Systému v prostředí LČR

Při implementaci Systému je nutné vždy zhodnotit dopady požadavků na provoz. Při začlenění do infrastruktury LČR je nezbytné brát v úvahu důsledné oddělení interní sítě a zabezpečení firewally. Z tohoto důvodu je nutné, aby při návrhu realizace byly stanoveny potřebné požadavky na úpravy provozní a bezpečnostní infrastruktury. Provoz aplikace respektuje architekturu řešení, především vyžadovanou lokalizaci jednotlivých funkčních komponent v odpovídajících bezpečnostních zónách, např. Systém poskytující data do internetu musí být umístěn v samostatně odděleném segmentu sítě (DMZ) apod. a to dle členění jednotlivých bezpečnostních zón a zón důvěryhodnosti (trust zones) v LČR

3.4.7. Ochrana Systému typu webové aplikace.

Části Systému typu webová aplikace musí být chráněny proti nejčastějším útokům, které byly identifikovány nezávislým společenstvím OWASP (http:www.owasp.org) tím, že se při vývoji použijí principy definované dle této metodiky v aktuálním znění. Podle dobré vžité praxe musí být pozornost věnována především následujícím známým zranitelnostem:

- Cross Site Scripting (XSS). XSS je metoda narušení WWW stránek využitím bezpečnostních chyb ve skriptech (především neošetřené vstupy).
- Injection útoky. SQL injection je technika napadnutí databázové vrstvy programu vsunutím (injection) kódu přes neošetřený vstup a vykonání vlastního, pozměněného, SQL dotazu. Vedle SQL injection existují též další podobné scénáře s jiným cílem, např. shell command injection, LDAP injection atd.
- UmístěníVzdálené spuštění kódu a to buď vlivem zranitelnosti v samotném webovém serveru, použitém frameworku či logice ve webové aplikaci.
- Nezabezpečený přímý popis objektu. Zranitelnosti této kategorie umožňují útočníkovi získat informace o jednotlivých objektech cílové aplikace bez patřičné autentizace.
- Cross Site Request Forgery (CSRF). CSFR je technika, která umožňuje útočníkovi podvrhnout formulář na jiné stránce nebo pomocí některých HTTP metod přesměrovat prohlížeč oběti na skript zpracovávající legitimní formulář aplikace s daty, která můžou oběť poškodit.

- Únik informací nebo nedostatečné řízení chyb. Zranitelnosti tohoto typu útočníkovi zpřístupňují v případě chybového stavu aplikace informace, které lze později použít k lepšímu plánování útoku.
- Špatná autentizace a správa relace. Zranitelnosti tohoto typu umožňují útok na přihlašovací části aplikace či úplné obcházení přihlašovacího systému.
- Nezabezpečené kryptografické úložiště. Zranitelnosti tohoto typu můžou způsobit kompromitaci privátního šifrovacího klíče jedné či obou stran spojení.
- Nezabezpečená komunikace. Zranitelnosti tohoto typu umožňují útočníkům odchytávat komunikaci, která jim není určená, a provádět též aktivní útoky typu Man-in-the-Middle.
- Chybné zamezení URL přístupu. V případě, že aplikace umožňuje neautentizovaný přístup i ke stránkám, ke kterým by měl být přístup jen po příslušné autentizaci, je možnou zranitelností situace, kdy takto odkazovaná stránka zobrazí některé informace, které by měly být přístupné jen konkrétním autorizovaným uživatelům, či systémové informace citlivého charakteru.
- Nezabezpečené vzdálené volání API. Chybí standardizovaný protokol pro autorizaci a autentizaci, komunikace není šifrována, nepoužívají se digitálně podepsané tokeny, případně není omezena množina předávaných informací. Loginy a hesla jsou staticky uvedena přímo v aplikaci.

Zjištění některé z výše uvedených bezpečnostních zranitelností, případně jiných zranitelností známých v okamžiku vývoje webové aplikace je považováno za vadu vytvořené aplikace.

Ochrana proti CSRF je na LČR implementována globálně, tedy v rámci celého prostředí, a to na infrastrukturní i aplikační vrstvě, a to dle možných dopadů a potřebnosti. Požadavky musí být konfrontovány s touto koncepcí a musí být rozhodnuto, zda ochrana proti CSRF bude řešena v rámci požadavku nebo v rámci globálních opatření. Také je nutné brát zřetel na to, jaká opatření již byla implementována nebo v jakém stavu je jejich realizace a zda se opatření navrhovaná v aplikaci nepřekrývají nebo nejsou ve vzájemném rozporu s již přijatými nebo aplikovanými opatřeními na jiných vrstvách nebo v jiných oblastech. Ochrana proti CSRF musí být samostatně konzultována s OICT.

Při použití XML komunikace by měly být prováděné tyto kontroly:

- Početní a délkové limity
  1. Kontrola délky vstupních dat, kontroluje se maximální velikost zpracovávaného souboru v bytech na definovanou velikost.
  2. Maximální počet atributů v elementu
  3. Maximální počet namespaces, namespace prefixů a obecně všech lokálních jmen v XML dokumentu
  4. Maximální délka jména elementu
  5. Maximální délka jména atributu
  6. Kontrola maximální délky komentáře, Délka komentáře větší než definovaný počet znaků
  7. Maximální délka identifikátoru namespace (URI)
- Znakové sady
  8. Konzistence deklarací (atribut „charset“ v HTTP request hlavičce „Content-Type“, BOM na začátku dat a atribut „encoding“ v hlavičce XML)
  9. Přítomnost netisknutelných znaků
- Escaping
  10. Escaping validních znaků (např. „A“ místo „A“, též např. „Я“ místo „Я“, pokud je použitý encoding některý z UTF apod.)
  11. Použití znaku „&“ mimo escape sekvenci

12. Použití znaků „““ (uvozovky – ASCII 34), „’“ (apostrof – 39), „<“ a „>“ mimo místa, kde mají syntaktický význam
13. Kontrola správného ohraničení CDATA sekcí (pokud se vůbec mohou vyskytovat, pokud ne, tak rovnou odmítat XML zprávy, které CDATA obsahují)
    - Přítomnost XML External Entity v DTD
14. Upřesnit text ve vztahu k XSD + obecný pravidla XML fw na agri.
15. Kontrola na překročení maximálního povoleného počtu zanoření. Doporučeno 20 úrovní.

Při použití JSON formátu pro výměnu dat by měly být prováděné minimálně tyto kontroly:

- maximální velikost zprávy
- maximální délka názvu klíče
- neunikátní klíče
- maximální počet elementů
- maximální úroveň vnoření
- maximální velikost pole (myšleno array, nikoli field)
- komentáře, pokud jsou zakázané nebo limitované velikostí
- limit objemu whitespace (tabulátory, mezery, odřádkování)
- kontrola striktní syntaxe a struktury JSON dokumentu (některé parsery v aplikacích ledacos tolerují)
- kontrola kanonické formy nebo provedení kanonizace (pokud je požadována)
- kontrola obsahu (jména klíčů, hodnoty) na sekvence XSS či SQLi (s možností vypnout per element – nemusí být datově transparentní a někdy může hodnota naopak záměrně obsahovat renderované HTML)
- provádí se kontrola syntaxe kódu JSON – parser pro RFC4627
- validace key value, metoda zjišťuje, zda hodnoty použité v key value odpovídají typu definované hodnoty (numeric,boolean apod.)
  Případně doplnit hodnoty. Oddělit ws a klient versus aplikace. Odkaz na standart.

3.4.8. Antivirová ochrana

Pro implementaci Systému musí být navržen způsob antivirové ochrany především pomocí stávajících řešení používaných v prostředí LČR. Dodavatel zhodnotí všechny směry a vstupy dat do Systému a navrhne způsob antivirové kontroly. Vezme přitom v úvahu existující antivirové nástroje LČR a jejich standardy.

Pro jakýkoliv upload souboru bude použito povinně služba antivirové detekce.

3.4.9. Testování Systému

Testování Systému musí probíhat v souladu s metodologií vývoje.
Integrační testy, systémové, zátěžové a akceptační testy musí vždy probíhat ve vyhrazeném testovacím prostředí nebo módu, tak aby nemohla být narušena činnost produkčních systémů. Penetrační a bezpečnostní testy probíhají i na produkčním prostředí a provádí je nezávislý auditor, tak aby byl zajištěn atribut nestrannosti. Scénáře penetračních a bezpečnostních testů musí být předem odsouhlaseny manažerem kybernetické bezpečnosti za stranu LČR. Penetrační nebo bezpečnostní testování včetně konfiguračního review, musí být provedeno po implementaci Systému a musí ověřit správnost nastavení celého prostředí.

Testovací údaje (data) musí být dostatečně chráněna a kontrolována. Pokud je nezbytné využít k testování provozní data, upřednostní se použití již neplatných dat. Při výběru provozních dat k testování z provozních databází je nutné použít maskování položek, které nejsou pro potřeby testování nezbytné.
Pokud je nutné použít platná provozní data, musí být dodrženy následující zásady:

- postupy kontroly přístupu platné pro provozní data musí být uplatněny i pro testovací data,
- každé kopírování provozních dat do testovacího prostředí musí být autorizováno souhlasem garanta IS a schválením pracovním týmem (například ve schváleném zápisu z pracovního týmu nebo HTP),
- neveřejné informace musí být okamžitě po ukončení testů odstraněny z testovaného prostředí bezpečným způsobem, aby nebyla možná jejich dodatečná obnova,

kopírování a užití provozních dat musí být zaznamenáváno do auditních záznamů.

V případě požadavku objednatele mohou být vyvíjené aplikace prověřeny nástrojem pro analýzu zdrojového kódu a nástrojem na zjišťování zranitelností. Součástí akceptace musí být prohlášení o provedení těchto testů a jejich výsledky. Dodavatel Systému poskytne prohlášení o provedení těchto testů, které bude obsahovat minimálně tyto položky:

- Datum provedení testu
- Použitá testovací metodika a metodika scoringu
- Název nástroje použitého pro testování, pokud byl použit
- Konfigurace profilu pro testování
- Testovací protokol
- Výsledky testování, navržení protiopatření
- Shrnutí výsledku testování a závěrečná zpráva
- Osobní odpovědnost – jména odpovědných osob

Při realizaci změn musí být prováděno vždy uživatelské testování, výkonnostní a integrační testy a další viz tato kapitola, dle potřeby.

3.4.10. Patch management

Odstranění zranitelnosti musí probíhat i v dodavatelské i provozní fázi. V provozní fázi nejméně 1x za dva měsíce nebo dle plánu patch managementu pro daný Systém nebo v případě dodání nových komponent při změnových řízeních apod. Dodavatel Systému navrhne v rámci patch managementu testování Systému a jeho běhu na OS s nově vydávanými bezpečnostními záplatami. V dodavatelské fázi je možné s ohledem na implementaci Systému udělit výjimku z patch managementu. Výjimku uděluje Manažer kybernetické bezpečnosti.

Týká se požadavků realizujících dodávky nových modulů nebo větších částí, v těchto případech ověřuje dodavatel jejich zranitelnost při nasazení. Dodavatel je povinen používat při vývoji poslední stabilní verze OS, nástrojů a dalších komponent dle aktuální verze používané na LČR.

3.4.11. Komunikace

Způsob řešení integrace na externí systémy.
Pokud Systém využívá data nebo služby externích systémů, měla by být jejich integrace provedena prostřednictvím centrální komunikační sběrnice ESB.

Komunikace s externími systémy musí být rozdělena podle stupně zabezpečení na:

- Zabezpečený kanál přenosu (šifrování dat) s povinnou úrovní zabezpečení koncových bodů Systému na úrovni infrastruktury.
- Šifrování dat pro přenos a autorizací uživatele v rámci Systému.
- Zajištění šifrování nebo náhradu citlivých dat na úrovni poskytovatelských a konzumentských systémů pomocí end to end metody při přenosu dat pomocí centrální komunikační sběrnice. Např. pole nesoucí osobní data je nahrazeno identifikátorem nebo pomocí hash.

V případě požadavku na vznik komunikace mezi 2 systémy, bez ohledu na to, zda bude komunikace skrze WS nebo databázový link je nezbytné v Požadavku:

- Definovat rozsah vyměňovaných dat
- V případě WS definovat strukturu request a response
- V případě databázového pohledu definovat strukturu tabulek, k nimž má mít druhý systém přístup
- V případě, že komunikace vyžaduje zřízení nového účtu pro přístup k datům, pak je nezbytné tento požadavek definovat (tj. příjemce dat, rozsah přístupu po věcné stránce)
- Pro databázové pohledy je nutné dodržet princip least privilege, musí být stanoven rozsah přístupu v DB, autentizace pomocí standardních nástrojů DB, používá se pouze read-only přístup.
- Výjimky povoluje OKB.

3.4.12. Fyzická bezpečnost a požadavky na infrastrukturu datových center.

Požadavky na fyzickou bezpečnost, nároky na HW platformu a infrastrukturu datových center jsou definovány v aktuální Směrnici OICT

Požadavky na Infrastrukturu datových center.

Infrastruktura, musí splňovat požadavky zejména na:
• Zajištění ochrany prostor – bezpečnostní perimetr,
• Zabezpečení přístupu osob,
• Nezávislý zdroj elektrického proudu /UPS/,
• Přesná klimatizace prostor,
• Datové rozvody dle technických norem,
• Bezpečnost kabelových rozvodů,
• Zabezpečení a ochranu datové centra vč. elektronické zabezpečovací signalizace,
• Vícenásobné kapacitní připojení k internetu,
• Možnost vybudování vlastní optické konektivity.

Týká se pouze požadavků realizujících dodávky s dopadem do fyzické bezpečnosti. (Např. změny HW a jeho umístění apod.)

3.4.13. Dokumentace

Dodávaná dokumentace Systému obsahuje položku bezpečnostní dokumentace.
Ta musí obsahovat popis všech relevantních bezpečnostních atributů pro dodávku Systému. Jedná se o popis v tomto standardu výše uvedených relevantních požadavků pro daný systém a to především o popis těchto bezpečnostních opatření (jsou-li relevantní):

a. Řízení přístupu, role, autentizace a autorizace, druhy a správa účtů,
b. Omezení oprávnění (princip minimálních oprávnění),
c. Proces řízení účtů (přidělování/odebírání, vytváření/rušení)
d. Auditní mechanismy, napojení na centrální logování (Syslog, SNP TRAP, Textový soubor, JDBC, Microsoft Event Log…),

e. Šifrování,
f. Zabezpečení webového rozhraní, je-li součástí systému,
g. Certifikační autority a PKI,
h. Zajištění integrity dat,
i. Zajištění dostupnosti dat (redundance, cluster, HA…),
j. Zálohování, způsob, rozvrh,
k. Obnovení ze zálohy (DRP) včetně předpokládané doby obnovy.
l. Předpokládá se, že existuje síťové schéma, komunikační schéma a zdrojový kód.

Kromě těchto atributů je vyžadováno schéma začlenění Systému a komunikační mapa na úrovni L2-L3 topologie. Dodavatel si vyžádá podkladové materiály, tak aby byl schopen vytvořit tuto komunikační mapu a schéma, a to již jako součást návrhu Systému v případě, že je to součástí změny a ta obsahuje dopad na síťovou architekturu. Pokud se tato změna provádí na infrastruktuře LČR, předá dodavatel všechny relevantní požadavky na síťovou architekturu.

Bezpečnostní dokumentace není vyžadována jako samostatný dokument, ale jednotlivé bezpečnostní funkce jsou popsané a jsou součástí Provozně technické dokumentace.
Změny musí být zavedeny v režimu změn v aplikaci MS Word.

Tabulka 1 - seznam zkratek

Termín	**Význam**
AAA	Autentizace – Autorizace – Acounting (Auditing), tedy ověření identity - přidělení oprávnění – vytvoření záznamu o přístupu
BOM	(Byte order mark, česky přibližně „označení pořadí bajtů“) je znak hexadecimálně zapsaný jako FEFF
DB	Databáze
Externisté	Všechny osoby a externí strany vykonávající práce pro LČR na základě smluvního vztahu
Firewall	Zařízení nebo řešení pro řízení a zabezpečování síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti
Helpdesk	Specializované *oddělení Objednatele* zajišťující komplexně uživatelskou podporu
Internisté	Zaměstnanci a to jak v pracovním poměru, tak i zaměstnaných na základě dohod o pracích konaných mimo pracovní poměr
ITSM	IT service management – řízení úrovně poskytovaných Služeb především, nikoliv však výhradně, v rozsahu doporučeném ITIL
LDAP	Lightweight Directory Access Protocol - protokol pro ukládání a přístup k datům na adresářovém serveru nebo přímo zkratka pro adresářový server
Maintenance	Služby a aktivity, poskytované výrobcem Systému nebo jeho komponent, potřebné pro udržení Systému v provozuschopném stavu v souladu s dohodnutými parametry a zajišťující kompatibilitu Systému s komponentami ICT Objednatele
LČR	Lesy České republiky, s.p.
Objednatel, Zadavatel	osoba, která je jako Objednatel definovaná v záhlaví Smlouvy
OS	Operační systém
Rozhraní Systému	integrační a komunikační rozhraní Systému prezentované vnějším rozhraním hraničního (posledního) aktivního síťového prvku pod správou Zhotovitel/Dodavatele, tvořícího rozhraní mezi sítí Zhotovitel/Dodavatele a vnější komunikační infrastrukturou

Servisní okno	časový interval definovaný Objednatelem a zakotvený v dokumentaci, pro potřeby odstávek
SIEM	Security incident & event management – systém pro správu incidentů a událostí
Smlouva	Smlouva o poskytnutí řešení „Systém“ uzavřená mezi Objednatelem a Zhotovitel/Dodavatelem
SSL	Secure Sockets Layer - vrstva která poskytuje zabezpečení komunikace šifrováním a autentizaci komunikujících stran
Standardní SW (SSW)	softwarové vybavení třetích stran dodané v rámci Smlouvy, na základě kterého byl zhotoven Systém, které nebylo vyvinuto Zhotovitel/Dodavatelem a není aplikační SW komponentou Systému vyvinutou v rámci Smlouvy
Systém	Vyvíjená nebo vyvíjená a dodávaná aplikace, informační systém na míru nebo podobný program a řešení, a dále i komerční software
WS	Webová služba
Zhotovitel/Dodavatel	osoba, která je jako Zhotovitel/Dodavatel definovaná v záhlaví Smlouvy