OSON/OREG/006/16

MEMORANDUM
o spolupráci při rozvoji Národní databáze brownfieldů
uzavřené mezi
Agenturou pro podporu podnikání a investic CzechInvest
a
Jihočeským krajem

(dále jen „**Memorandum**“)

KUJCP01ID07B

Agentura pro podporu podnikání a investic CzechInvest,
státní příspěvková organizace,
se sídlem: Štěpánská 15, 120 00 Praha,
IČ: 71377999
zastoupena: Mgr. Ing. Karel Kučera, generální ředitel

(dále uváděna jako “**CzechInvest**”)

a

Jihočeský kraj
se sídlem: U Zimního stadionu 1952/2, 370 76 České Budějovice
IČ: 70890650
zastoupen: Mgr. Jiřím Zimolou, hejtmanem

(dále uváděn jako „**Kraj**“)

(dále obě společně uváděny jako „**Strany**“)

vedeny snahou o navázání spolupráce v oblasti podpory a rozvoje investic v nevyužívaných průmyslových lokalitách, tzv. brownfieldech, se strany dohodly na tomto Memorandu:

Úvodní ustanovení

CzechInvest se dlouhodobě zabývá problematikou nevyužívaných průmyslových lokalit, tzv. brownfieldů (dále jen „**brownfield**“). Na základě Vyhledávací studie pro lokalizaci brownfieldů a následné Národní strategie regenerace brownfieldů byla vytvořena Národní databáze brownfieldů (dále jen „**NDTB**“), která eviduje ucelené informace o lokalitách vhodných pro regeneraci a investiční záměry domácích i zahraničních investorů. Smyslem NDTB je zjednodušit investorům práci s výběrem vhodné lokality pro podnikání v ČR, a tak přispět k navrácení života na území, která člověk využil a pak opustil.

Kraj dlouhodobě mapuje a vytváří vlastní databázi brownfieldů na svém území s cílem rozšíření investičních příležitostí pro investory a regeneraci dlouhodobě nevyužívaných objektů v často velmi atraktivních lokalitách celého Jihočeského kraje.

I. Účel memoranda

1.1. Účelem memoranda je navázání a rozvoj spolupráce při naplňování NDTB informacemi o brownfieldech na území Jihočeského kraje.

II. Způsob spolupráce

2.1. CzechInvest poskytne Kraji administrovaný přístup do NDTB za účelem vkládání a editace informací o brownfieldech na území Jihočeského kraje. Podrobný technický popis přístupu do NDTB je přílohou tohoto memoranda.

2.2. Kraj je oprávněn vkládat a editovat data o brownfieldech umístěných na území kraje, a to bez možnosti jejich uvedení ve veřejné části NDTB. O změnách v záznamech musí informovat Agenturu CzechInvest.

2.3. Kraj nebude zřizovat vlastní databázi, ale na svých webových stránkách uvede odkaz na NDTB.

2.4. CzechInvest má právo kontroly údajů vložených Krajem a jejich zveřejnění ve veřejné části NDTB na adrese www.brownfieldy.cz.

2.5. CzechInvest poskytne Kraji know-how v otázce mapování lokalit brownfields pro Vyhledávací studii Jihočeského kraje.

2.6. CzechInvest vypracuje přehled nabízených lokalit brownfields v Jihočeském kraji na vyžádání Jihočeského kraje.

III. Odpovědné osoby

3.1. Strany se dohodly na stanovení odpovědných osob pro naplňování cílů tohoto memoranda a pro technické záležitosti provozování NDTB :

Za CzechInvest
Ing. Vladimíra Formanová email:vladimira.formanova@czechinvest.org,
tel.:+420 296 342 534

Za Jihočeský kraj:
Ing. Luboš Průcha, email: pruchal@kraj-jihoceky.cz, tel.: +420 386 720 214
Bc. Lucie Matysková, email: matyskova@kraj-jihocesky.cz, tel: +420 386 720 422

3.2. Osoba odpovědná za naplňování účelu smlouvy za Kraj určí nejvýše tři osoby, kterým bude povolen/zrušen administrativní přístup do NDTB. Tyto osoby budou mít právo vzdáleného přístupu do NDTB včetně vkládání a editace dat o brownfieldech umístěných na území Jihočeského kraje do neveřejné části, a to bez možnosti jejich uvedení ve veřejné části NDTB.

3.3. Administrovaný přístup do NDTB bude oprávněným osobám povolen/zrušen na základě písemné žádosti osoby uvedené v bodu 3.1. Memoranda zaslané CzechInvestu. Přístup do NDTB bude oprávněným osobám povolen po proškolení práce s NDTB pracovníkem CzechInvestu. Vzor žádosti o povolení/zrušení přístupu tvoří přílohu č. 2 smlouvy a je její nedílnou součástí.

3.4. Osoba s právem přístupu do NDTB je povinna dodržovat bezpečnostní požadavky dle dokumentu „Etalon minimální bezpečnosti pro smluvní partnery", který tvoří přílohu č. 3 smlouvy a je její nedílnou součástí.

IV. Zacházení s důvěrnými informacemi

4.1. CzechInvest se zaručuje, že zabezpečí důvěrnost údajů obdržených od Kraje v rámci tohoto Memoranda a nebude užívat tyto údaje pro jiné účely nežli pro účely, které byly výslovně ujednány.

4.2. Kraj se zaručuje, že zabezpečí důvěrnost údajů obdržených od CzechInvestu v rámci tohoto Memoranda a nebude užívat tyto údaje pro jiné účely nežli pro účely, které byly výslovně ujednány.

4.3. Kraj může používat data z NDTB pouze pro prezentaci Jihočeského kraje. Kraj nesmí předávat kontakty na majitele nemovitostí z NDTB.

4.4. Plnění tohoto závazku nebude od stran vyžadováno v případě, že je kterákoli z nich na základě svých příslušných vnitřních předpisů nebo na základě rozhodnutí soudního orgánu nebo jiného státního orgánu ze zákona povinna tomuto orgánu nebo třetí straně poskytnout informace týkající se tohoto memoranda.

V. Posilování spolupráce

5.1. Strany společně prohlašují, že v okamžiku, kdy to strany uznají za vhodné, provedou přezkoumání vzájemné spolupráce a budou jednat o možnostech úpravy či rozšíření této spolupráce za účelem naplňování cílů tohoto memoranda.

VI. Trvání a platnost memoranda

6.1. Toto Memorandum vstupuje v platnost dnem jeho podepsání oběma stranami a je uzavíráno na dobu určitou, tj. 6 měsíců ode dne, kdy vstoupilo v platnost.

6.2. Toto Memorandum bude automaticky prodlouženo o dalších dvanáct (12) měsíců, pokud se jedna ze stran nerozhodne jinak. Kterákoli ze stran má právo kdykoliv vypovědět Memorandum písemnou výpovědí s dvouměsíční (2) výpovědní lhůtou. Výpovědní lhůta počne běžet dnem doručení písemné výpovědi druhé straně.

VII. Závěrečná ustanovení

7.1. Toto memorandum může být změněno nebo doplněno pouze písemnými vzestupně číslovanými dodatky podepsanými oběma stranami.

7.2. Toto memorandum se vyhotovuje ve čtyřech (4) vyhotoveních, z nichž dvě (2) obdrží CzechInvest a dvě (2) vyhotovení obdrží Kraj.

7.3. CzechInvest souhlasí se zveřejněním tohoto memoranda a prohlašuje, že neobsahuje údaje, které tvoří předmět jeho obchodního tajemství podle § 504 zákona č. 89/2012 Sb., občanský zákoník.

7.4. Obě strany výslovně prohlašují, že toto memorandum je projevem jejich pravé a svobodné vůle, uzavřené nikoliv v tísni nebo za nápadně nevýhodných podmínek.

7.5. Uzavření tohoto memoranda bylo schváleno usnesením Rady Jihočeského kraje č. 56/2016/RK-80 ze dne 28.01.2016.

V Praze dne: 22. 3. 2016

Za CzechInvest:

[redacted]

Mgr. Ing. Karel Kučera,
generální ředitel
Agentura pro podporu podnikání a investic CzechInvest

V Českých Budějovicích dne: 19.02. 2016

Za Jihočeský kraj:

JIHOČESKÝ KRAJ

Mgr. Jiří Zimola
hejtman Jihočeského kraje

Příloha č. 1
Technický popis přístupu do NDTB, vkládání a editace dat.

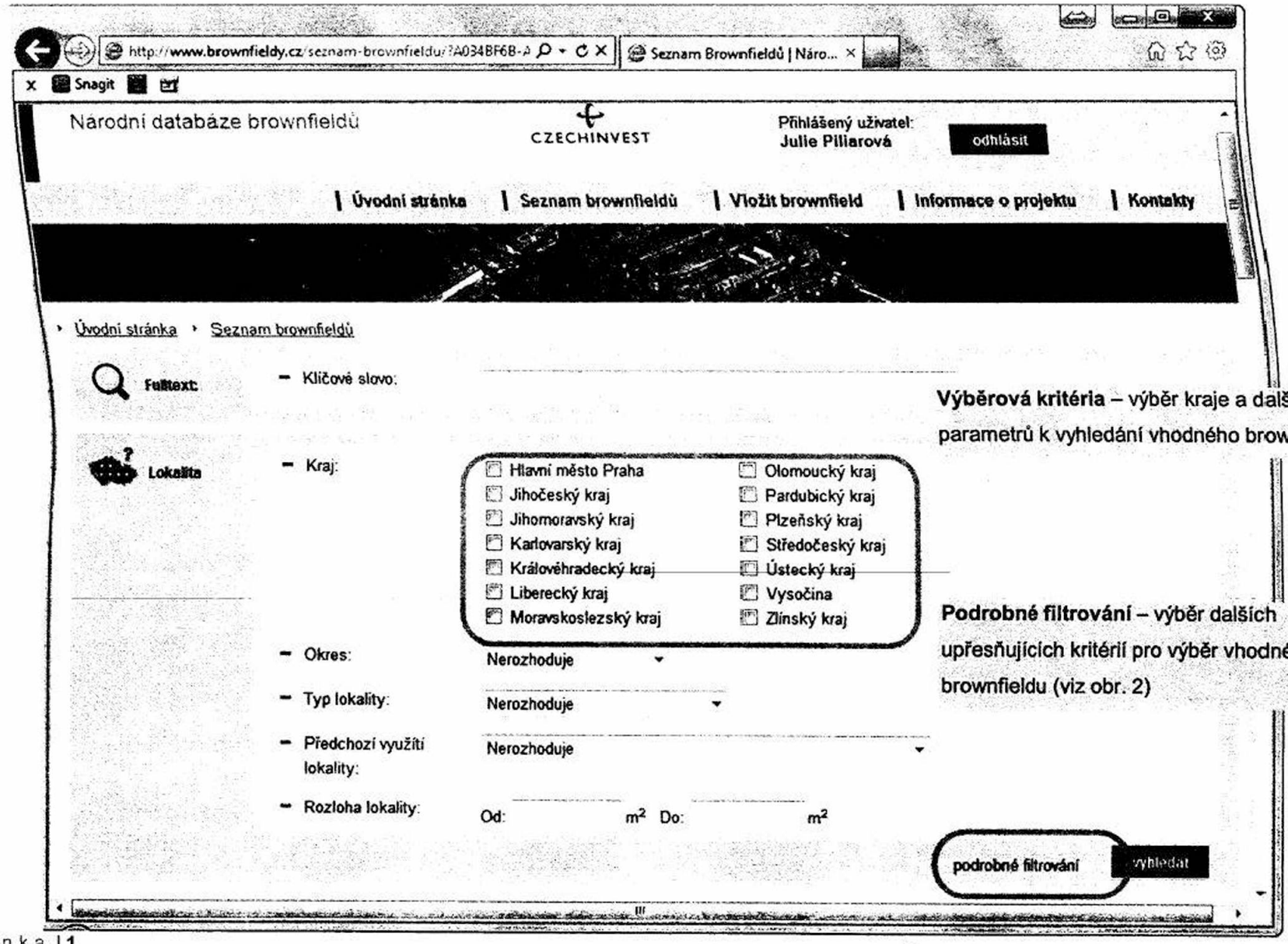
Příloha č. 2
Žádost o povolení/zrušení administrovaného přístupu do NDTB

Příloha č. 3:
Etalon minimální bezpečnosti pro smluvní partnery.

A. Uživatelská část

CZECHINVEST
Agentura pro podporu podnikání a investic

Náhled vyhledávácí části www.brownfieldy.cz



Výběrová kritéria – výběr kraje a dalších parametrů k vyhledání vhodného brownfieldu

Podrobné filtrování – výběr dalších upřesňujících kritérií pro výběr vhodného brownfieldu (viz obr. 2)

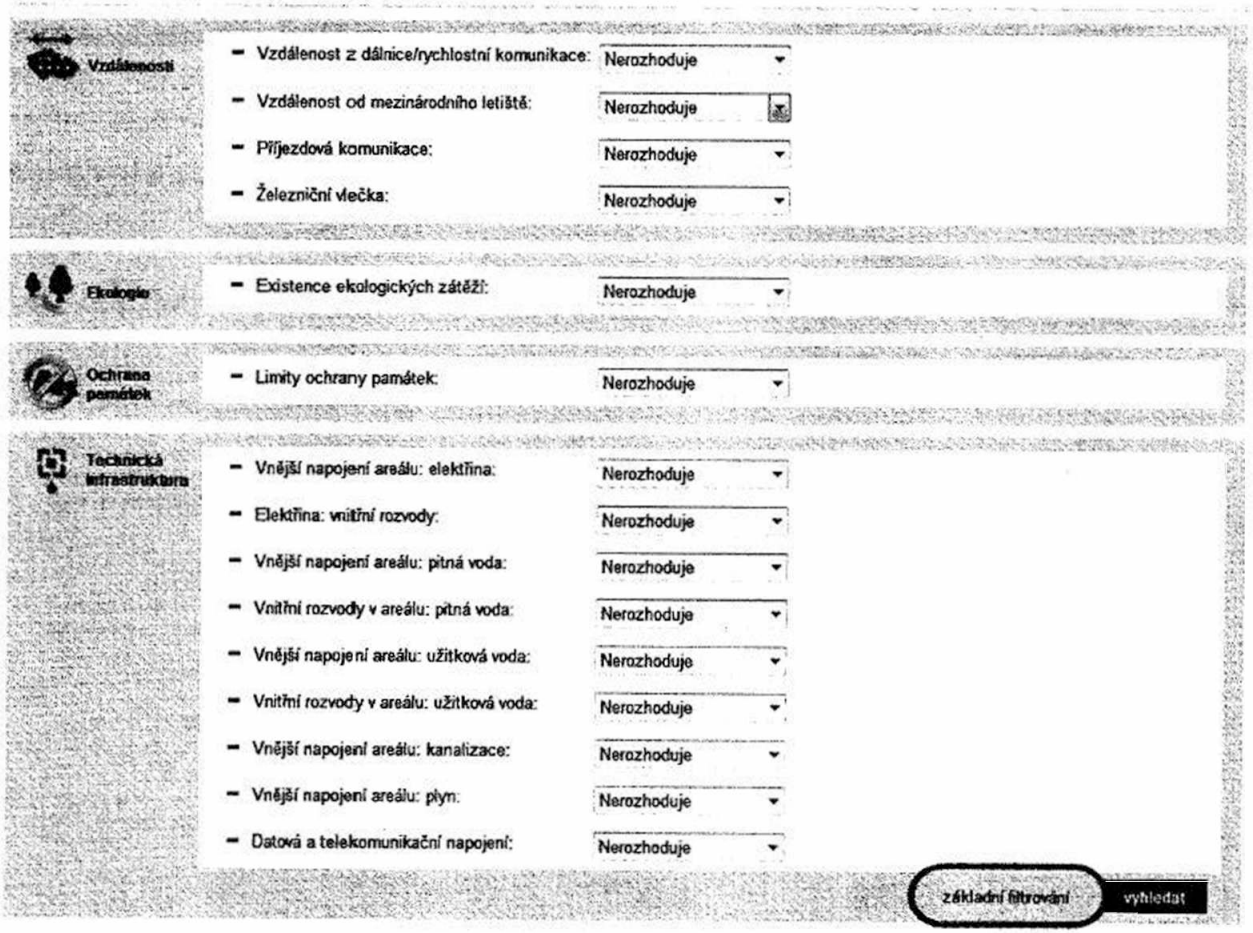
Příloha č. 1

Náhled po rozkliknutí odkazu „podrobné vyhledávání“

Náhled pro běžné uživatele – návštěvníky webu

Náhled je stejný jak pro přihlášené, tak nepřihlášené uživatele.

Brownfieldy lze vybírat z několika různých kritérií (kraj, okres, lokality – viz obr. 1)



Náhled po rozkliknutí kritéria **„podrobné filtrování“**

Vložit brownfield – již vyžadováno přihlášení / registrace uživatele.

Konec odd

B. Část určená pro editaci Brownfieldů

Pro vložení brownfieldu je již nutné přihlášení / registrace uživatele.

Uživatel, který již vložil nějaké záznamy prostřednictvím www.brownfieldy.cz, uvidí jen ty brownfieldy, které vložil.

Uživatel s přiřazenými právy (pracovník krajského úřadu) uvidí navíc veškeré záznamy spadající do jeho kraje (dále jen „právo editace"). Tato práva jsou přidělována CzechInvestem na základě žádosti (viz Memorandum a příslušné přílohy).

B. Část určená pro editaci Brownfieldů

CZECHINVEST
Agentura pro podporu podnikání a investic

Uživatel v této části („Vložit brownfield) s těmito právy vidí i **brownfieldy nepublikované** (tj. brownfieldy, které jsou rozpracované), informace o stavu jednotlivých záznamů jsou uvedeny v náhledu brownfieldu (viz následující screeny).

Publikovaný brownfield (ukazuje se tedy všem návštěvníkům webu www.brownfieldy.cz)

- **Název brownfieldu:** Zámek Horní Police
  Datum vložení: 20.12.2007
  Kraj: Liberecký kraj
  Stav brownfieldu: Publikováno *(případná editace brownfield depublikuje do doby schválení správcem)*
  Datum poslední změny: 11.11.2011

editovat náhled

Neublikovaný brownfield (ukazuje se pouze uživatelům s právem editace a pouze v části „Vložit brownfield)

- **Název brownfieldu:** Tovární areál Kateřinská, Liberec
  Datum vložení: 20.12.2007
  Kraj: Liberecký kraj
  Stav brownfieldu: Rozpracováno
  Datum poslední změny: 29.11.2011

editovat náhled

Podrobnější funkcionalita bude předmětem zaškolení uživatelů / pracovníků jednotlivých krajů, kteří budou s tímto editačním systémem pracovat.

B. Část určená pro editaci Brownfieldů

CZECHINVEST
Agentura pro podporu podnikání a investic

Editované záznamy na www.brownfieldy.cz:

Editované záznamy na www.brownfieldy.cz jsou vždy v kategorii „depublikované" – tj. nejsou vidět v seznamu brownfieldů pro běžné uživatele. Úpravou již publikovaného záznamu dojde automaticky k jeho depublikaci.

Publikovat záznamy mohou pouze pracovníci CzechInvestu, z odboru RPN.

PŘÍLOHA č. 2

Příloha č. 3 – Příloha č. 2 Smlouvy: Žádost o povolení/zrušení administrovaného přístupu do NDTB

Údaje o žadateli pro přístup na www.brownfieldy.cz – editační část

Žadatel – kraj:	
Název úřadu:	
Sídlo úřadu:	
Město:	
PSČ:	
Telefon:	

Údaje o žadateli o přístup (osoba zodpovědná za editaci záznamů na www.brownfieldy.cz):	
Jméno a příjmení, titul:	
Funkce:	
Telefon:	
Email[1]:	

Datum a podpis žadatele:

.....
.....

Datum a podpis osoby oprávněné jednat za Úřad ..... kraje:

.....
.....

Vyplňuje CzechInvest:	
Doručeno do CzechInvestu / č.j.:	
Přístup zřízen dne:	
Podpis oprávněné osoby za zřízení přístupu:	

---

[1] Email je současně přihlašovacím jménem na portále www.brownfieldy.cz

Příloha č. 3 – Příloha č. 2 Smlouvy: Žádost o povolení/zrušení administrovaného přístupu do NDTB

Žádost o zrušení přístupu na www.brownfieldy.cz

Jméno a příjmení, titul:	
Email:	

Datum a podpis osoby oprávněné jednat za Úřad ..... kraje:

.....
.....

Vyplňuje CzechInvest:	
Doručeno do CzechInvestu / č.j.:	
Přístup zrušen dne:	
Podpis oprávněné osoby za zrušení přístupu:	

ETALON MINIMÁLNÍ BEZPEČNOSTI PRO SMLUVNÍ PARTNERY

Agentury pro podporu podnikání a investic

CzechInvest

Veřejný dokument – určen pro smluvní partnery CzechInvestu

OBSAH:

ČÁST I – ÚČEL A ZÁVAZNOST

Etalon Minimální bezpečnosti pro dodavatele CI tvoří soubor pravidel a postupů, který vymezuje způsob a požadovanou úroveň bezpečnosti, vymezení aktiv a způsob jejich zajištění, týkající se obchodních společností se smluvním vztahem k CI.

Dodržování pravidel uvedených v tomto dokumentu je povinné pro všechny partnery spolupracující na smluvní bázi s CI, jejich zaměstnanci či osoby spolupracující se smluvními partnery (dále jen „smluvní partneři"), kterých se dotýká problematika bezpečnosti.

Používané i nově zaváděné informační systémy v rámci CI musí být upraveny, vyvíjeny a vybírány tak, aby splňovaly zásady bezpečnosti v souladu s tímto dokumentem.

Tento dokument je pro smluvní partnery CI veřejný.

ČÁST II – CÍLE DOKUMENTU

Bezpečnost je ochrana informací, systémů a služeb proti živelním událostem, lidským omylům a úmyslné manipulaci s cílem snížit pravděpodobnost a dopad bezpečnostních incidentů na minimum.

Cílem Etalonu minimální bezpečnosti pro dodavatele CI je obecně:

a) Specifikovat jasné zásady bezpečnosti CI pro dodavatele;
b) Zabránit porušení platných právních předpisů ČR;
c) Zamezit, příp. minimalizovat možnost finanční a majetkové újmy;
d) Zabránit neautorizovanému přístupu k informacím CI;
e) Umožnit provádění kontroly přístupu k informacím;
f) Zajistit dostupnost informací pro oprávněné uživatele i procesy;
g) Zabránit neautorizované modifikaci či zneužití dat nebo jiných aktiv a umožnit ověření původu informací;
h) Definovat základní pravidla rozvoje a výběru nových používaných prostředků a technologií (vývoj zabezpečovacích prostředků, vlastnosti používaných aplikací a operačních systémů);
i) Umožnit sledování a hodnocení stavu bezpečnosti.

ČÁST III – OBECNÉ POVINNOSTI

Mezi odpovědnosti smluvních partnerů patří zejména:

a) Dodržování platných bezpečnostních ustanovení a právních předpisů;
b) Využívání uživatelských systémů tak, jak bylo stanoveno vlastníkem informací (CzechInvest);
c) Používání informačních aktiv CI pouze v souladu s rozsahem přístupových oprávnění a pouze ke schváleným účelům;
d) Zajištění ochrany svých autentizačních údajů (login, heslo, identifikační předmět);
e) Odpovědnost za každý přístup k informacím, provedený prostřednictvím jejich autentizacích údajů;
f) Respektování všech bezpečnostních opatření a procedur určených vlastníkem informací;
g) Nerozšiřování dat bez souhlasu vlastníka informací nebo jeho nadřízeného.

ČÁST IV – BEZPEČNOST HW, SW A KOMUNIKACE

Smluvní partneři CI musí chránit aktiva CI, která používají ke své práci či k výkonu pro CI, a zabránit podle svých nejlepších možností a schopností jejich poškození, zneužití nebo odcizení.

4.1 Pracovní stanice, notebooky

Při práci na koncových uživatelských pracovištích CI musí být splněny nejméně následující bezpečnostní zásady:

a) Použití počítače CI musí být umožněno pouze oprávněné osobě;
b) Je zakázáno připojovat vlastní počítače do vnitřní sítě CI bez vědomí odboru informatiky CI;
c) Pracovní stanice nesmí být ponechány bez dozoru zapnuté a s přihlášeným uživatelem; je třeba přinejmenším použít heslem chráněného spořiče obrazovky;
d) Počítač smluvního partnera, který má být připojen do vnitřní sítě CI, musí mít instalován a spuštěn systém pro ochranu před škodlivými programy (antivirový program) v nejnovější verzi programu i virové databáze;
e) Smluvní partner je povinen chránit vybavení CI, udržovat okolo sebe bezpečné pracovní prostředí; v blízkosti výpočetní techniky je zakázáno jíst, pít a kouřit;
f) V případě ukončení práce se zařízením je smluvní partner povinen provést odhlášení od systému, aby se zamezilo zneužití jeho přístupových práv.

4.2 Využívání internetu

Systémy v CI vztahující se k počítačové síti, internetu a intranetu, včetně počítačového vybavení, programů, operačních systémů, médií pro ukládání dat, schránek elektronické pošty CI, možností prohlížení internetových stránek a zdrojů přístupných na FTP jsou vlastnictvím CI. Tyto systémy jsou používány pro pracovní účely tak, aby sloužily zájmům CI a jejím klientům při normální činnosti.

Smluvní partneři mají dovoleno používat internetové připojení do a z vnitřní sítě CI pouze za účelem pracovních záležitostí. Způsob připojení do vnitřní sítě CI a autentizace musí být předem dohodnuta s odborem IT CI a obsažena ve smlouvě. Obecně by měla platit povinnost oznámit předem datum a čas přihlášení k vnitřnímu prostředí a následně ukončení práce ve vnitřním prostředí CI.

ČÁST V – BEZPEČNOST SYSTÉMŮ IT

U vyvíjených nebo dodávaných informačních systémů musí být zjištěna níže uvedená pravidla:

5.1 Využívání internetu

a) Aplikace musí být vytvářeny tak, aby znemožnily přístup bez zadání hesla.
b) Uživatel aplikace musí být nucen si heslo pravidelně měnit.
c) Aplikace musí být vytvořena tak, aby byl počet neúspěšných pokusů o přihlášení omezen. Po třech neúspěšných pokusech o přihlášení musí být další zadávání dočasně ochromeno nebo spojení rozpojeno.
d) Pokud je při přihlašování do aplikace některá část chybná, nesmí být uživateli poskytnuta informace, ve kterém z údajů je chyba.
e) V případě, že je povolen přístup do aplikace, v níž určuje vstupní heslo administrátor, je povinností autora aplikace vynutit si změnu tohoto inicializačního hesla.
f) Všichni uživatelé musí při své činnosti užívat jedinečný identifikátor (přihlašovací jméno) tak, aby bylo možné vysledovat odpovědnost jednotlivců za prováděné činnosti.
g) Smluvní partner smí používat jedno přihlašovací jméno pro několik svých zaměstnanců, přičemž smluvní partner odpovídá za veškeré úkony provedené v informačním systému CI pod těmito identifikátory.
h) Systém správy hesel musí být podpořen efektivním a interaktivním vybavením, které prosazuje kvalitu hesel.

5.2 Monitorování používání systému a přístupů k systému

V informačních systémech musí být pořizovány auditní záznamy obsahující:

a) Identifikaci uživatele;
b) Datum a čas přihlášení a odhlášení;
c) Identifikaci místa, odkud se uživatel přihlašovat (pokud je to možné);
d) Záznamy o přístupu (úspěšném i neúspěšném).

5.3 Řízení přístupu k informačním systémům

a) Před umožněním přístupu musí být každý uživatel identifikován a autentizován;
b) Informační systém by měl po určité době nečinnosti uživatele (doporučeno 15 minut) tohoto uživatele odhlásit;
c) Po určitém množství neúspěšných autentizačních pokusů (doporučeno 3) se musí ukončit přihlašovací procedura;
d) V případě neúspěšné autentizace nesmí systém poskytnout uživateli informaci o tom, která část autentizace je chybná;
e) Pro každého uživatele systému musí být možné identifikovat, jaká má přístupová práva;
f) Pro každý prostředek musí být možné vytvořit seznam uživatelů, kteří mají přístupová práva k tomuto prostředku s rozlišením druhu přístupových práv (čtení, úprava atd.);
g) Informační systém musí mít mechanismus pro odejmutí všech přístupových práv konkrétnímu uživateli nebo skupině.

ČÁST VI – BEZPEČNOST DAT

6.1 Využívání internetu

Data vstupující do systémů musí být kontrolována tak, aby byla zajištění jejich správnost. V aplikacích se musí evidovat identifikátor uživatele nebo procesu, který změny nebo pořízení provedl.

Pro kontrolu dat je nezbytné aplikovat opatření:

a) Vstupní kontrola (neplatné znaky, rozsah, přetečení, kompletnost, souvislost…);
b) Kontrola vnitřního zpracování dat;
c) Kontrola oprávněnosti běhu programů;
d) Kontrola integrity dat;

e) Kontrola obsahu generovaných dat.

Opatření musí zahrnovat i popis postupu při zjištění chyby.

Pokud CI usoudí, že vytvářená aplikace by měla podporovat kryptografii, je nezbytné, aby byly podporovány mezinárodně uznávané standardy a dodrženy právní předpisy České republiky.

6.2 Data předávaná smluvním partnerům

Jedná se o informace předávané z CI smluvnímu partnerovi na jakémkoliv nosiči, zejména jakékoliv listiny, interní dokumenty CI, CD-ROM, diskety, pevné disky počítačů a jiné nebo zasílané e-mailem. Smluvní partner musí nakládat s předávanými daty v souladu s ustanoveními tohoto dokumentu.

a) Předávání dat musí být vymezeno ve smlouvě (struktura dat, způsob předávání, způsob ochrany, periodicita, oprávněné osoby atd.), a musí probíhat bezpečným způsobem.
b) Uchovávání a případné zpracování dat u smluvního partnera musí být prováděno tak, aby byla zajištěna jejich dostatečná ochrana před neoprávněným přístupem a aby bylo znemožněno jejich zneužití.
c) Zodpovědnost za dostatečnou ochranu předávaných dat má smluvní partner.
d) Je nutno dbát na bezpečnost likvidace již nepotřebných dat, případně médií s daty. Pro likvidaci medií nesoucích neveřejné informace musí být zvolena metoda, která zaručuje, že takto zlikvidované informace není možno běžně dostupnými prostředky obnovit (skartovače, SW skartovače).
e) Každé nové předávání dat na smluvním základě je vhodné již při tvorbě smlouvy konzultovat s Manažerem bezpečnosti IT.
f) Smluvní partner si nesmí sám stahovat žádná data z IS CI; vytváření souborů musí provést oprávněný zaměstnanec CI a teprve takto vytvořená data smí být (na smluvním základě) předána partnerovi.

ČÁST VII – BEZPEČNOST DODÁVEK A SLUŽEB

7.1 Vývoj softwaru smluvními partnery

Vývoj software musí probíhat:

a) Legálním softwarem;
b) Na testovacím prostředí odděleném od prostředí produkčního;

c) Na testovacích datech, která nejsou převzata z provozní databáze; pokud je nutné použít data z provozní databáze, je nutné je anonymizovat;

d) Tak, že migrace do provozního prostředí může být provedena až po akceptaci výsledků testů ve vývojovém prostředí a formalizovaném a doložitelném odsouhlasení.

Přístup dodavatele do IS CI:

a) Vzdálený přístup dodavatele může být povolen pouze do vývojového a testovacího prostředí za podmínek dohodnutých s odborem IT CI. Výjimky může povolit pouze Manažer bezpečnosti informací CI.

b) Lokální přístup dodavatele do provozního prostředí musí být zcela výjimečný a bude povolen pouze v odůvodněných případech. Tento přístup musí probíhat ve zvláštním režimu dohledu ze strany odboru IT CI nebo oprávněných uživatelů, vždy ale až po povolení odboru IT CI na základě zdůvodnění dodavatele.

c) Přístup dodavatele do IS CI (testovacího i provozního prostředí) může být použit pouze pro zpracování zadané oprávněným pracovníkem CI.

7.2 Dodávka software

Dodávka software musí být řádně smluvně zajištěna a průběžně kontrolována a dokumentována.

U veškerého dodávaného programového vybavení musí být zřejmé, zda se jedná o volně šířený software nebo program podléhající licenční a registrační politice.

7.3 Dodávka hardware

Dodávka hardware musí být řádně smluvně zajištěna a průběžně kontrolována a dokumentována. O každé dodávce musí existovat kromě účetních dokladů i předávací protokol podepsaný dodavatelem a odběratelem. Způsob předání závisí na konkrétním produktu a na smlouvě s dodavatelem.

Každé nové zařízení musí být otestováno, než bude akceptováno a zařazeno do produkčního prostředí.

7.4 Dodávka služeb

Dodávka služeb musí být řádně smluvně zajištěna a průběžně kontrolována a dokumentována. Způsob předání závisí na konkrétní službě a na smluvních podmínkách dohodnutých ve smlouvě s dodavatelem.

7.4.1 Dodávka HW a SW

Smluvní partneři zajišťující servis hardware nebo software jsou na základě smlouvy oprávněni pohybovat se na neveřejných místech v CI pouze s vědomím odboru IT CI.

7.4.2 Ostatní služby

Smluvní partneři zajišťující ostatní služby, např. úklid, ostrahu, atd. jsou na základě smlouvy oprávněni pohybovat se na neveřejných místech v CI. Při svém pohybu musí dbát bezpečnostních pravidel a pokynů odboru správy majetku a autoprovozu (THS).

7.5 Dokumentace o provedené práci

Nedílnou součástí dodávky hardware, software nebo služeb tam, kde to má smysl, je projektová a bezpečnostní dokumentace. Rozsah a náplň dokumentace musí být specifikován ve smlouvě s dodavatelem. Chybějící, neúplná nebo neaktuální dokumentace je důvodem k reklamaci dodávky a v krajním případě i důvodem odstoupení od smlouvy z důvodu jejího nenaplnění ze strany dodavatele.

7.6 Akceptace

Každý dodaný hardware, software nebo služba musí být plně a široce otestován, zda splňuje očekávané a smluvně definované parametry, a zda jeho používání nepředstavuje neočekávaná bezpečnostní rizika. Než bude systém předán do rutinního provozu, musí být formálně akceptován managementem a specialisty.

7.7 Outsourcing

Outsourcing musí být řádně smluvně zajištěn a průběžně kontrolován a dokumentován. Všechna externí zpracování neveřejných informací CI musí být smluvně ošetřena tak, aby byla zachována úroveň ochrany ve všech aspektech informační bezpečnosti podle požadavků CI a platných právních předpisů.

ČÁST VIII – FYZICKÁ BEZPEČNOST

Cílem fyzické bezpečnosti v oblasti IT je chránit prostředí, ve kterém se nacházejí aktiva CI, dále zabránit náhodnému i cílenému neautorizovanému přístupu, poškození nebo narušení aktiv v prostorách CI.

V CI jsou všechny oblasti rozděleny na oblasti pro veřejnost a oblasti neveřejné. V neveřejných oblastech není dovolen pohyb cizích osob bez doprovodu pracovníka CI a cizí osoba nesmí být zanechána bez dozoru v neveřejné oblasti, pokud tyt skutečnosti nejsou ošetřeny smlouvou.

8.1 Poskytování informací třetím stranám

Smluvní partneři jsou povinni dodržovat mlčenlivost o skutečnostech, které se dozvěděli při výkonu své činnosti v souladu s uzavřenou smlouvou v CI. Tato skutečnost musí být ošetřena smlouvou, ve které může být udělena výjimka např. pro účely reference.

Každé veřejné použití neveřejných informací CI (např. na veřejných vystoupeních, do publikací apod.) musí být schváleno vlastníkem těchto informací.

ČÁST VII – ZÁVĚREČNÁ USTANOVENÍ

Závažné porušení bezpečnostních standardů zavedených v CI bude klasifikována jako porušení smlouvy a CI a od smluvního partnera může být požadována náhrada vzniklé škody s ohledem na okolnosti vzniku škody.