1 Požadavky na soulad s legislativou a metodikou bezpečnosti

ID	Požadavek
1	Systém MUSÍ splňovat: - Povinnosti, vyplývající ze zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů, a z vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat pro informační systémy kritické informační infrastruktury, ve znění pozdějších předpisů, - Povinnosti, které bude nezbytné implementovat na základě Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2), budou naplněny po nabytí účinnosti nového ZoKB.
2	Systém MUSÍ zajistit soulad (nikoli certifikaci) s aktuální verzí ISMS, zejména s normou ISO/IEC 27001. - Normy rodiny ISO/IEC 27000 v aktuálních verzích budou v rámci vývoje Systému implementovány ve shodě se ZoKB a navazujícími vyhláškami z důvodu určení systému jako KII. Rozsah implementace normy rodiny ISO 27000 je v rámci Systému stanoven rozsahem kapitol 4 až 10 normy ISO/IEC 27001 a přílohy A této normy. V následujících etapách případného rozvoje Systému budou implementovány další normy nebo jejich části dle vzájemně odsouhlaseného harmonogramu.

2 Řízení bezpečnosti informací

ID	Požadavek
1	Dodavatel MUSÍ zajistit soulad navrženého řešení se Systémem řízení bezpečnosti informací, reprezentovaného souborem interních směrnic zadavatele (Příloha č. 1 RS DWH).
2	V rámci návrhu a implementace DWH MUSÍ být stanoven rozsah systému a stanovena odpovědnost za ochranu informací všech komponent systému.
3	Součástí implementace MUSÍ být příslušná bezpečnostní a provozní dokumentace, zpracovaná dle interní metodiky zadavatele (Příloha č. 1 RS DWH) určující pravidla pro dokumentaci v oblasti bezpečnosti informací.
4	Jako součást implementace MUSÍ být zpracována Analýza rizik dle metodologie NÚKIB, která bude obsahovat minimálně: - Identifikaci aktiv, jejich garantů a provozních požadavků (důvěrnost, dostupnost, integrita), - Identifikace rizik, hrozeb a zranitelností v rozsahu identifikovaných aktiv, - Způsob ochrany identifikovaných aktiv. Analýzu rizik bude řídit a metodicky zajišťovat zadavatel, případně jím určená třetí strana. Dodavatel systému MUSÍ: - Poskytnout součinnost během přípravy Analýzy, - Poskytnout informace a vstupy, nezbytné pro zpracování Analýzy rizik, - Zapracovat výstupy Analýzy rizik do návrhu prohlášení o aplikovatelnosti a plánu zvládání rizik, - Doplnit příslušné části bezpečnostní dokumentace dle metodiky Analýzy rizik, resp. metodik zadavatele na bezpečnostní dokumentaci informačních systémů.
5	Součástí implementace MUSÍ být začlenění procesů a projektových a provozních struktur do řízení organizační bezpečnosti dle interní metodiky Objednatele (Příloha č. 1 RS DWH). Příslušné bezpečnostní role pak MUSÍ být začleněny do konceptu oprávnění systému.

3 Řízení dodavatelů

ID	Požadavek
1	Dodavatel MUSÍ zajistit, že všechny jím zasmluvněné subjekty, které se budou účastnit návrhu, implementace a provozu DWH, se zaváží a budou dodržovat relevantní ustanovení zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících předpisů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů.
2	Dodavatel MUSÍ zajistit, aby všechny jím zasmluvněné subjekty, které se budou účastnit návrhu, implementace a provozu DWH, budou v souladu s požadavky vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů, a ve vzájemně odsouhlaseném rozsahu s Objednatelem dodržovat následující pravidla: - Během všech činností souvisejících s návrhem, implementací a podporou DWH budou dodržovat pravidla stanovená legislativními pravidly, - Nakládat s daty v souladu s jejich účelem a klasifikací, - Řídit přístup a nakládání s osobními údaji, - Dodržovat bezpečnostní politiky a bezpečnostní opatření ve formě organizačních a technických opatření, - Komunikovat o bezpečnostních událostech a incidentech, - Řídit bezpečnostní rizika, - Řídit kontinuitu provozu, - Předávat předem dohodnutou formou data, provozní údaje a informace vyžádané zadavatelem.

4 Aplikační bezpečnost

ID	Požadavek
1	Dodavatel musí v politice aplikační bezpečnosti dodržet požadavky na striktní oddělení testovacího prostředí od provozního prostředí. Žádné nasazení jakékoliv komponenty DWH nesmí být puštěno do provozního prostředí bez řádného otestování na testovacím prostředí.
2	Dodavatel musí navrhnout v politice aplikační bezpečnosti systém označování upgradů, patchů a dalších komponent tak aby bylo jasné, které z nich naplňují požadavek vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů, na „významnou změnu“. Takovéto komponenty pak musí dodavatel otestovat zranitelnosti a doložit výsledky tohoto testování. Nasazení takovéto komponenty je možné až po schválení výsledků testů dodavatelem. Samotné testování musí proběhnout vzájemně schválenou metodou.
3	Součástí implementace systému MUSÍ být také specifikace a nasazení postupů a prostředí, sloužících pro minimalizaci rizik spojených s řízením životního cyklu řešení DWH, zejména tedy způsob vyhledávání a získávání nových verzí nebo záplat provozovaných komponent, řízení vývoje zákaznického kódu, postup nasazení a pravidla přenosu mezi jednotlivými provozními prostředími, způsob a pravidla pro testování funkcionalit a procesy řízení přechodu do produkčního prostředí.
4	Součástí návrhu systému MUSÍ být kromě definice komponent a funkcionalit také definice postupů pro zajištění kontinuity činností a služeb, podporovaných informačním systémem. Součástí návrhu MUSÍ být také postupy, nástroje a funkcionality sloužící ke sledování a vyhodnocení dostupnosti služeb, zvládání výpadků a nedostupností a zotavení po chybě.
5	Pro zajištění důvěryhodnosti a integrity zpracovávaných dat MUSÍ systém zajistit nástroje a komponenty, které zajistí ochranu dat, komunikací a průkaznost identity uživatele, zejména: - Nástroje pro šifrování a ochranu informací, přičemž použitá šifra musí být v souladu s platným pokynem NÚKIB na typ a délku šifrovacího klíče, - Nástroje pro ověření průkaznosti a nezpochybnitelnosti dat, - Infrastrukturu PKI pro potřeby příchozí i odchozí komunikace, - Nástroje pro správu a řízení životního cyklu certifikátů, a to jak pro potřeby certifikátů využívaných a spravovaných systémem, tak certifikátů uživatelů.

5 Provozní bezpečnost – Požadavky na záznam a sledování bezpečnostně významných událostí

5.1 Obchodní metadata

Obchodními metadaty rozumíme dodatečné informace, které vznikají, obvykle automaticky, jako součást funkcionalit založení, změny, ukončení nebo jiné manipulace s obchodními daty (také se někdy používá termín změnové doklady). Obchodní data neboli business data jsou vlastní, kmenová data datové báze. V případě DWH se jedná o veškeré zpracovávané primární datové objekty, jejich atributy a číselníky. Jejich primárním účelem je zaznamenat, a následně zpřístupnit, historii konkrétního datového objektu, resp. manipulace s ním. Součástí takových metadat jsou např. historické hodnoty, identifikace osob, které s obchodními data manipulovali, způsob jejich vzniku nebo zániku atd.

ID	Požadavek
1	Systém MUSÍ zajistit, aby obchodní metadata byla vždy referována na příslušná obchodní data, a to až na úroveň konkrétního záznamu.
2	Systém MUSÍ zajistit, aby obchodní metadata byla automaticky zaznamenávána systémem.
3	Systém MUSÍ zajistit, aby v případě, že původcem změny je jiný systém, byly příslušné atributy součástí předávaných dat.
4	Systém MUSÍ zajistit, aby obchodní metadata byla ukládána tak, aby byla procesně i technicky nezávislá na uložení vlastních obchodních dat. Nezávislé zpracování a uložení musí být zajištěno tak, aby manipulace s obchodními daty, zejména: - Pořízení a uložení dat, - Vyhledávání, vyhodnocení a reporting, - Archivace, skartace (resp. výmaz), byla proveditelná bez přístupu na referovaná obchodní data, resp. aby obchodní data nebyla manipulací s obchodními metadaty postižena.
5	Systém MUSÍ zajistit, aby obchodní metadata byla udržovaná minimálně v následujícím rozsahu: - Reference na konkrétní záznam obchodních dat, - Identifikace komponenty, která iniciovala změnu (preferujeme identifikaci zdrojové komponenty na základě autentizace rozhraní, nikoliv pouhým vyplněním atributu na úrovni rozhraní), - Druh změny (založení, změna, ukončení platnosti atd.), - Datum a čas provedené změny zdrojového systému, - Datum a čas provedené změny (automaticky přebíraný systémový čas v rámci celého prostředí DWH), - Identifikace uživatele – původce změny, - Předmět změny (data změnového dokladu).

5.2 Technická metadata – logy

Technickými metadaty (logy) rozumíme data, která automaticky generuje informační systém jako záznam své činnosti. Jejich primárním účelem je:

1) Provozní metadata:
   a) Zaznamenat informace důležité pro sledování a vyhodnocení stavu systému, jeho provozních parametrů a technického stavu,
   b) Zaznamenat informace nutné pro vyhodnocení technických procesů, které nejsou bezprostředně vázané na zpracování obchodních dat (profylaxe systému),
   c) Zaznamenat informace nutné pro vyhodnocení technických procesů, které jsou bezprostředně vázané na zpracování obchodních dat, nicméně jejich vyhodnocení není možné navázat na konkrétní datový objekt (protože v tom případě by se jednalo o obchodní metadata) – např. zpracování dávkových vstupů, zpráv a dat doručených přes rozhraní atd.
2) Bezpečnostní metadata:

a) Zaznamenat systémové informace, nutné k bezpečnostnímu sledování a vyhodnocení,
b) Zaznamenat činnost uživatelů, nutné k vyhodnocení přístupu k osobním údajům.

5.3 Provozní metadata

ID	Požadavek
1	Systém MUSÍ zajistit, aby provozní metadata byla generována ke všem významným událostem systému, zejména: - Každé zpracování dat, které nebude zaznamenáno ve formě obchodních nebo bezpečnostních metadat (např. dávkově zpracovávané úlohy, importy nebo exporty dat), - Každé volání rozhraní. Pro rozhraní, kdy DWH bude přímo komunikovat s externími systémy mimo prostředí FS, systém MUSÍ zajistit uchování originálů zpráv. Pro komunikaci s interními systémy FS není uchování zpráv vyžadováno, - Informace o vytížení systému na úrovni kontinuálních informací o čerpání zdrojů a volných rezervách. Systém MŮŽE evidovat čerpání zdrojů na úrovni zdrojů přiřazených jednotlivým zpracovávaným úlohám.
2	Systém MUSÍ zajistit, aby provozní metadata byla uchovávána tak, aby manipulace s nimi (např. kontrola, vyhledávání, reporting a vykazování, export, archivace nebo výmaz) neměly dopad na dostupnost a integritu ostatních dat spravovaných systémem (za předpokladu, že záznam vlastní změny je uložen na úrovni obchodních metadat).

5.4 Bezpečnostní metadata

ID	Požadavek
1	Systém MUSÍ zajistit, aby bezpečnostní metadata byla udržována minimálně v následujícím rozsahu: - Přihlášení a odhlášení uživatelů, - Neúspěšné pokusy o přihlášení uživatelů, - Neúspěšné pokusy uživatele o spuštění operací, ke kterým nemá oprávnění, pokud je možné, aby se uživatel o spuštění pokusil, - Změny privilegií a bezpečnostních atributů uživatelů nebo uživatelských rolí, - Změny nastavení bezpečnostních, systémových parametrů, - Změny přístupových práv, - Historie provedených operací uživatelů, včetně pasivních přístupů, - Všechny spouštěné procesy s uvedením kdo, kdy a jaký proces spustil a s jakými parametry, - Auditní záznam aktivit uživatele musí mimo jiné zahrnovat minimálně: o identifikaci uživatele (uživatelský účet), o identifikaci terminálu v případě interního uživatele nebo skutečnou IP adresu zařízení v případě externího uživatele, pokud je to technicky možné, o datum a čas, o úplné údaje o události (např. typ události, stará/nová hodnota, výsledek události atd.), o systém logování bude podporovat nastavení úrovně závažnosti logů, a to minimálně ve 4 úrovních.

Samostatnou částí řešení bude záznam přístupu na data. Vzhledem k typu dat zpracovávaných v DWH MŮŽE zadavatel pro vybrané komponenty nebo části systému požadovat registraci veškerých dotazů na data, a to jak úspěšných, tak neúspěšných (pravděpodobně na úrovni záznamu konkrétních dotazů na data). Tento požadavek je zde definován jako obecný, vzhledem k rozsahu zaznamenávaných údajů bude nutné zajistit jej prostřednictvím systémových nástrojů použité platformy. Proto bude konkrétní rozsah specifikován jako součást návrhu technického řešení DWH.

6 Správa logů

Systém MUSÍ zajistit využití nástroje pro centrální sběr a vyhodnocení logů, který bude součástí dodávaných služeb infrastruktury. Samotný log musí obsahovat minimálně informace definované na něj ve vyhlášce č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů.

7 Požadavky na bezpečnostní monitoring

Zadavatel požaduje, aby DWH zajistil generování, centralizaci a zpřístupnění bezpečnostně významných informací pro potřeby Zadavatele (administrátorů a bezpečnostních analytiků) a dohledových orgánů tak, aby bylo možné zajistit povinnosti provozovatele kritické infomační infrastruktury.

Zadavatel uvádí, že prostřednictvím SPCSS, s. p. provozuje vlastní systém bezpečnostního monitoringu (SOC). DWH MUSÍ zajistit integraci a předávání všech bezpečnostně relevantních dat do prostředí SOC, a to bezpečně, průkazně a bez zbytečného zpoždění.

ID	Požadavek
1	Systém MUSÍ poskytovat nástroje pro sledování stavu informačního systému jako celku, stavu jednotlivých komponent i činností jednotlivých procesů a uživatelů.
2	Systém MUSÍ zajistit předávání všech relevantních informací, zejména všechny typů logů, do prostředí bezpečnostního monitoringu zadavatele, a to bezpečně, průkazně a bez zbytečného zpoždění. Logy musí mít minimální podobu definovanou vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů.
3	Dodavatel MUSÍ navrhnout a implementovat procesy, které zajistí plnou integraci na bezpečnostní procesy zadavatele a Poskytovatele infrastruktury při identifikaci Kybernetických bezpečnostních událostí tak aby Manažer kybernetické bezpečnosti zadavatele mohl provést bezodkladnou klasifikaci případných incidentů a ty procesovat podle vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů.

8 Požadavky na ochranu před škodlivým kódem

ID	Požadavek
1	Systém MUSÍ zajistit kontrolu veškeré komunikace s ohledem na výskyt rizikového nebo škodlivého obsahu. Systém MUSÍ být navržen tak, aby podmínky a rozsah kontrol bylo možné během provozu doplňovat nebo měnit.
2	Systém MUSÍ zajistit příjem pouze vybraných typů dokumentů. Systém MUSÍ zajistit antivirovou kontrolu a kontrolu škodlivého kódu přijímaných a odesílaných dokumentů dle jejich typu. Antivirovou kontrolu a kontrolu škodlivého kódu lze realizovat i samostatným dedikovaným modulem.
3	Systém MUSÍ zajistit kontrolu předávaných nebo přebíraných strukturovaných dat s ohledem na přítomnost škodlivého kódu. Antivirovou kontrolu a kontrolu škodlivého kódu lze realizovat i samostatným dedikovaným modulem.
4	Systém MUSÍ zajistit ochranu kódu DWH pomoc elektronického podpisu deployovaného kódu, minimálně pro všechny SW komponenty distribuované mimo provozní prostředí DWH.

9 Požadavky na správu certifikátů a autentizačních údajů

ID	Požadavek
1	Zabezpečení konfiguračních dat (např. přístupové údaje do dalších systémů, různá hesla v konfiguraci atd.) MUSÍ být zajištěno dostatečně silnou šifrou a v souladu s metodickým pokynem NÚKIB pro použití kryptografických prostředků.
2	Pro autentizační data, uložená v informačním systému, MUSÍ být dostatečně dobře zajištěna důvěrnost a integrita (např. prostřednictvím relevantní a bezpečné hash funkce).
3	Řešení bude povinně používat pro uložení klíčů určených pro elektronický podpis, resp. pečeť, vytvářené centrálními aplikacemi HSM modul, který zadavatel využívá jako součást infrastrukturních služeb Poskytovatele infrastruktury.
4	Řešení MUSÍ zajistit soulad s eIDAS.

9.1 Secure by Design

Návrh řešení DWH musí respektovat princip „Secure by Design". Pojem „Secure by Design", (Bezpečný již od návrhu) se používá v oblasti vývoje softwarových produktů a představuje postup, při kterém je kybernetická bezpečnost produktu zohledňována už během počátečních fází vývoje, tj. na úrovni návrhu architektury softwarového produktu. Princip „Secure by Design" zahrnuje různé techniky, například provedení důkladné analýzy hrozeb navrhovaného software, návrh bezpečné architektury a implementaci bezpečnostních kontrol.

Uplatnění principu „Secure by Design" popisuje odkazovaný dokument „Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software (cisa.gov)"[1] připravený ve spolupráci řady bezpečnostních složek a kyberbezpečnostních úřadů, od amerických, přes australského, izraelské, německé až po český NÚKIB. Dokument obsahuje základní principy kybernetické bezpečnosti pro organizace zabývající se vývojem software. S ohledem na počet autorů je dokument do jisté míry obecný, resp. přináší zejména základní principy, jak k této oblasti přistupovat.

9.2 Bezpečnostní architektura

Rámcový model bezpečnostní architektury je znázorněn na následujícím obrázku.