Standardní operační postup (SOP)

ČNRDD/A02/verze01
Politika informační bezpečnosti Českého národního registru dárců dřeně o.p.s (WISP)

1. Účel a předmět

Politika informační bezpečnosti definuje postupy ČNRDD, jejichž cílem je:

- chránit informace před vnitřními i zevními hrozbami, úmyslnými i náhodnými
- zajistit, že všichni pracovníci si jsou vědomí svých odpovědností při práci a ohraně informací
- efektivně řídit rizika bezpečnosti informací a zavádět přiměřená opatření
- chránit ČNRDD před nevhodným využíváním informací

Pravidla pro informační bezpečnost se týkají všech organizačních složek ČNRDD, ale také partnerů a spolupracujících organizací.

2. Pojmy

2.1. ČNRDD využívá pro zpracování a uchování dat informační systém, jehož součástí je několik aplikací. Dodavatelem a správcem systému je Západočeská Univerzita v Plzni (dodavatel informačních technologií, ZČU). Dodavatel se řídí bezpečnostními standardy WMDA a jeho zodpovědnosti jsou smluvně definovány.

2.1. Cílem činností prováděných v rámci informační bezpečnosti je chránit informace před neautorizovaným použitím, nechtěnou modifikací či ztrátou. Hlavní aspekty informační bezpečnosti zahrnují:

- důvěrnost: k informacím přistupují pouze autorizované osoby
- integrita: je zajištěna správnost a kompletnost informací a procesů jejich zpracování
- dostupnost: autorizované osoby mají přístup k informacím, když je potřebují
- spolehlivost: je zajištěn soulad mezi zamýšleným chováním a výsledky
- návaznost použití: s informacemi se zachází v souladu s legislativou, standardy WMDA a smlouvami s dodavateli

3. Organizace informační bezpečnosti

3.1. Pověřenec pro ochranu osobních údajů (DPO)

- Kompetence a povinnosti pověřence pro ochranu osobních údajů jsou stanoveny v SOP ČNRDD/A01 *Ochrana osobních údajů v Českém národním registru dárců dřeně o.p.s. ve vztahu k požadavkům GDPR* a zahrnují mimo jiné:
- poskytování poradenství vedení i zaměstnancům registru ohledně ochrany informací a osobních údajů
- posuzování souladu s právními předpisy v oblasti informační bezpečnosti a ochrany osobních údajů

- vyhodnocování rizik bezpečnosti informací a rizik pro práva subjektů osobních údajů
- posuzování smluv s dodavateli, se kterými se sdílí osobní údaje dárců, a jejich souladu s politikou informační bezpečnosti
- kontakty s příslušným národním dozorovým úřadem a kontakty pro WMDA *Security and Privacy Committee* a ostatní DPO partnerských registrů
- systematická spolupráce s manažerem informační bezpečnosti

3.2. Manažer informační bezpečnosti (MBI)
- ověřuje harmonizaci aktivit ČNRDD s platnou legislativou týkající se informační bezpečnosti
- odpovídá za dohled nad organizací informační bezpečnosti, hodnocení informačních rizik a příslušných kontrolních procesů
- poskytuje při vývoji a provozování IT systémů ČNRDD konsultace v případech, které mohou mít vliv na informační bezpečnost
- ověřuje, že jsou pracovníci proškoleni v problematice informační bezpečnosti
- spolupracuje v oblasti informační bezpečnosti s Oddělením bezpečnosti IT služeb ZČU
- zodpovídá za provádění pravidelných auditů informační bezpečnosti

3.3. Správci informačního systému
- správci informačního systému ČNRDD jsou pracovníci Západočeské university, která je dodavatelem informačních technologií a zajišťuje provoz serveru a poskytovaných služeb
- správce je povinen chránit poskytnuté přístupové k serverům a programovým prostředkům před zneužitím 3 stranou
- za ČNRDD je pověřený ke komunikaci se správci/dodavatelem manažer informační bezpečnosti

3.4. Uživatelé aplikací informačního systému
- musí být seznámeni s pravidly informační bezpečnosti a dodržovat je
- musí hlásit incidenty porušení informační bezpečnosti MBI/DPO
- všechny informace obsahující osobní údaje musí předávat v zabezpečené podobě (anonymizace, pseudoanonymizace, šifrování)

3.5. Správci operačního systému
- správci operačního systému jsou zaměstnanci jednotlivých organizací (ZČU, FN Plzeň, KC ČNRDD, nemocnice dárcovských center) pověření svou organizací k údržbě jejího hardware a IT infrastruktury

4. Přístupy uživatelů do informačních systémů ČNRDD

4.1. Každý pracovník zacházející s aplikacemi ČNRDD je unikátně identifikovatelný svými přístupovými údaji (konto, heslo).

4.2. Přidělování přístupů pro uživatele jednotlivých softwarových aplikací ČNRDD je dáno jejich pracovním zařazením (viz SOP ČNRDD/M02) a řídí se níže uvedenými pravidly:

4.2.1. Operátor KC – oprávnění přístupu do aplikace RDKD/EMDIS a CEKOOR smí být uděleno administrátorem systému na požadavek vedoucího KC, oficiálně vedeného na webových stránkách registru ČNRDD

4.2.2. Operátor DC – oprávnění přístupu do aplikace CEDAR a specifického DC smí být uděleno administrátorem systému na požadavek vedoucího specifického DC, oficiálně vedeného na webových stránkách registru ČNRDD

4.2.3. Správce DC (operátor všech DC) – oprávnění přístupu do aplikace CEDAR smí být uděleno administrátorem systému pouze na požadavek ředitele ČNRDD

4.2.4. Operátor HLA laboratoře ČNRDD – oprávnění přístupu do aplikace CELAB smí být uděleno administrátorem systému na požadavek vedoucího HLA laboratoře, oficiálně vedeného na webových stránkách registru ČNRDD

4.3. Udělování oprávnění v rámci ZČU – ADMIN

4.3.1. Administrátorské přístupy k jednotlivých aplikacím do systému mají privilegovaný uživatel, správce aplikace a programátor v rámci údržby a vývoje informačního systému ČNRDD

4.3.1.1. privilegovaný uživatel má přístup k aplikacím ČNRDD a nastavení uživatelů

4.3.1.2. správce aplikace pravidelně zálohuje databázi a řeší případné problémy centrální databáze na serveru, nahrává nové verze programu, konfiguruje VPN

4.3.1.3. programátor vytváří a modifikuje program, vydává nové verze programu, je oprávněn k zásahu do programu i databáze

4.3.2. Přístupy do infomačního systému ČNRDD jsou přidělovány po schválení ředitele ČNRDD

4.3.3. Při odchodu nebo změně na pozici administrátora, resp. dostatečně privilegovaného uživatele, se vždy mění administrátorské přístupy.

4.4. Všichni ostatní pracovníci přistupují do aplikací v režimu standardního uživatele, administrátorské přístupy jsou vyhrazené správcům informačního systému (ZČU).

4.5. Pokud je to nutné vzhledem k zachování bezproblémového provozu serveru, mají kromě správce aplikací ZČU přístup definovaní pracovníci správy hostingu, servisu a údržby systému.

4.6. Pro všechny uživatele je nastaven systém rotace hesel, který požaduje pravidelnou změnu hesla.

4.7. Při ukončení změně pracovního zařazení nebo ukončení pracovního poměru se přístup uživatele do aplikací na požadavek odpovědného vedoucího pracovníka ČNRDD aktualizuje nebo případně ukončuje.

5. Zacházení s informacemi

5.1. Informace jsou kategorizovány na osobní, zdravotnické záznamy a systémové údaje (přístupy apod.)

5.2. Personální a technické zajištění informační bezpečnosti je definováno v SOP ČNRDD/M02 *Elektronické záznamy*, kde jsou stanoveny mimo jiné postupy pro:

- přístupová práva a zabezpečení
- validaci a údržbu databází
- testování, schvalování a vydávání nových verzí aplikací
- zachování integrity a unikátnosti záznamů
- práci s aplikacemi včetně verifikace záznamů
- zálohování databází

- řešení problémů a závady ve funkci aplikací
- trénink uživatelů

5.3. Pracovníci koordinačního/transplantačního centra pracují pouze s unikátním a přesně definovaným identifikačním kódem dárce (dle SOP ČNRDD/K02). Na základě tohoto identifikačního kódu je možné i zpětné vyhledání informací o produktech dárce.

6. Technická opatření informační bezpečnosti

6.1. Na všech pracovištích ČNRDD, na pracovištích ZČU i na jednotlivých dárcovských centrech jsou zavedená opatření omezující přístup nepovolaných osob.

6.2. Jakákoliv osoba, která není jednoznačně označena institucionální zaměstnaneckou jmenovkou umožňující přístup do prostor, musí být aktivně vyzvána k identifikaci a vysvětlení své přítomnosti.

6.3. Důvěrné informace nesmí být ponechány v případě nepřítomnosti pracovníka bez dozoru (nenechávat na stole, uložit do zamykatelné skříně, nebo za zamčené dveře).

6.4. Sever (technická infrastruktura) je umístěn u dodavatele informačních technologií ZČU, který zajišťuje provoz virtuální privátní sítě (VPN), instalace a aktualizace operačních systémů, zálohovaní apod.

6.4.1. Je oddělen server pro databázi, servery poskytující webové rozhraní, zároveň je oddělena infrastruktura pro provoz a testování.

6.4.2. Všechny servery jsou přístupné pouze přes VPN, přístup do VPN je řízen pomocí certifikátu umístěného na USB tokenu – přístupy podléhají dvoustupňové autentizaci a autorizaci.

6.4.3. Servery mají firewall na úrovni operačního systému, který je pravidelně aktualizován.

6.4.4. Všechny servery a databáze jsou pravidelně zálohovány.

6.4.5. Je zajištěno ochrana před selháním dodávky elektrického napájení – záložní zdroj UPS

6.5. Komunikace mimo informační systém probíhá šifrovaně pomocí SSH/TLS, OpenPGP.

7. Operační opatření informační bezpečnosti

7.1. Databáze informačního systému je v daných intervalech zálohována, probíhá pravidelná údržba a sleduje se systematicky její funkčnost. Zodpovídá správce informačního systému.

7.1.1. Průběžně se monitorují aktivity na úrovni technické i procesní – např. monitoring bezpečnostních záznamů, detekce možných průniků do systému, sledování a analýza logu chyb, kontrola datových toků (ustálenost), probíhají dílčí penetrační testy (databáze, web-testing, …).

7.1.2. V pravidelných intervalech (minimálně 3x ročně) probíhají u správce informačního systému preventivní prohlídky zaměřené na funkčnost výpočetní techniky a provádí se preventivní opatření před budoucími poruchami – dochází

k bezpečnostním aktualizacím, nasazování nových verzí využívaných a potřebné výměně hardwaru.

7.2. Jakékoliv slabiny databáze či aplikací (nestability, atypického chování nebo nefunkčnosti) zjištěné při běžném provozu nebo při hodnocení informační bezpečnosti (např. výstupy průběžného monitoringu, penetračních testů) se musí aktivně řešit, aby bylo bezpečnostní riziko odstraněno. Vydané opravy se vždy verifikují. Zodpovídá správce informačního systému.

7.3. Všechny záznamy v databázi jsou unikátní a aplikace jejich unikátnost kontrolují. Integrita dat se pravidelně kontroluje interními postupy dodavatele informačních technologií.

7.4. Při sdílení a přenosu informací mezi jednotlivými pracovišti ČNRDD nezajištěnými datovými kanály, musí být data šifrována dle kryptografického standardu OpenPGP.

7.5. Při sběru a dalším zpracováním kumulovaných dat musí být z datasetu odstraněny všechny osobní identifikátory.

7.6. Přístupy do aplikací jsou řízené, podléhají autorizaci a jsou umožněné pouze oprávněním pracovníkům s přidělenými přístupovými údaji.

8. Incidenty porušení informační bezpečnosti

8.1. Za incident informační bezpečnosti se považuje jakákoliv událost nebo podezření na událost, která může ohrozit nebo ohrozila data nebo informační systémy ČNRDD. Incidenty mohou pocházet zevnitř ČNRDD nebo z externích zdrojů a zahrnují:

- prozrazení osobních údajů (dárců)
- ztráta dat z důvodu technické či organizační chyby
- modifikace dat z důvodu technické či organizační chyby
- únik dat z důvodu technické či organizační chyby
- ztráta klíčenky/tokenu
- neautorizované přístupy (hackerské útoky)
- poškození způsobená škodlivým kódem
- phishingové emailové útoky
- porušení organizačních opatření

8.2. Jakékoliv podezření na porušení informační bezpečnosti musí pracovník hlásit ihned svému nadřízenému pracovníkovi, správci informačního systému.

8.3. Závažné incidenty se vždy oznamují řediteli a vedoucímu lékaři ČNRDD a také DPO MBI registru.

8.4. Při vzniku incidentu je správce informačního systému oprávněný přijmou nezbytná opatření k minimalizaci škod a ochraně dat ČNRDD:

- omezení funkčnosti aplikací, přístupu uživatelů atd. k zabránění dalších škod
- vyšetření incidentu a zjištění, zda došlo k porušení informační bezpečnosti
- informování dotčených uživatelů
- vyhodnocení ev. právních dopadů
- dokumentace nápravných a případných preventivních opatření

8.5. Podezřelé emaily (phishing) se řeší s příslušným pověřeným IT pracovníkem dané organizace (nemocnice, ČNRDD, ZČU).

8.6. Incidenty porušení informační bezpečnosti se sumarizují v ročním *Přezkoumání informační bezpečnosti vedením.*

9. Posuzování a ošetření rizik bezpečnosti informací

9.1. Posuzování rizik bezpečnosti informací

9.1.1. Rizika porušení informační bezpečnosti jsou posuzována v kontextu - zda se jedná o riziko narušení důvěrnosti, integrity, dostupnosti informací či možnou kombinaci dopadů a zároveň s čím je riziko spojeno, jako např. technická závada, typ útoku, porušení organizačních opatření, mimořádná událost atd.

9.1.2. Závažnost rizik a z nich vyplývajících možných incidentů je posuzována na základě svého významu z pohledu úniku dat, kde nejvyšší význam je kladen na míru možného úniku osobních dat.

- incident nesouvisející s možnou ztrátou či únikem dat
- incident související se ztrátou dat
- incident s možným únikem dat v rámci organizace
- incident s možným únikem dat mimo rámec organizace

9.1.3. Analýzu rizik informační bezpečnosti provádí pravidelně dodavatel informačních technologií, který zároveň přijímá vhodná opatření u procesů spojených s vyšším rizikem.

9.2. Ošetření rizik bezpečnosti informací

9.2.1. Technická a operační opatření bezpečnosti informací (kap. 6, 7) jsou pravidelně aktualizována či modifikována za účelem snížení pravděpodobnosti vzniku incidentů

9.2.2. Na základě definovaných typů rizik/incidentů jsou pro jednotlivé procesy plánována bezpečnostních opatření, které je možno aplikovat v případě vzniku incidentu, jako např.:

- organizační opatření
- obnova dat ze záloh
- odstavení serveru
- zablokování komunikace
- zrušení přístupových údajů
- revokace využívaného certifikátu
- aktualizace/modifikace aplikací

10. Kontinuální zlepšování informační bezpečnosti

10.1. Odpovědní pracovníci registru a dodavatele informačních technologií sledují legislativu týkající se informační bezpečnosti a soulad procedur registru s touto legislativou.

10.2. Cílem zlepšování informační bezpečnosti je implementace základních postupů stanovených normou ISO 27001.

10.3. Politika informační bezpečnosti se aktualizuje minimálně 1 x za 2 roky, musí být schválená vedením registru a musí s ní být seznámeni všichni pracovníci, kterých se dotýká.

11. Povinnosti pracovníků

11.1. Všichni pracovníci musí rozumět pravidlům a požadavkům informační bezpečnosti a řídit se standardy ČNRDD a WMDA.
11.2. Přístup do aplikací ČNRDD mají pouze pracovníci s přiděleným kontem, které je opravňuje k přístupu k určitým činnostem. Přístupová práva vyplývají z funkčního zařazení pracovníka. Blíže viz SOP ČNRDD/M02 *Elektronické záznamy*, kapitola *Přístupová práva a zabezpečení*.
11.3. Pracovníci jsou povinni přistupovat do aplikací pouze pod svým uživatelským kontem, musí uchovávat své přístupové údaje v tajnosti a zamezit možnosti jejich zneužití. Pracovníci jsou zodpovědní za akce provedené v aplikacích pod jejich přihlášením.
11.4. Pracovníci jsou zodpovědní za správnost dat vkládaných do aplikací a také za zneužití dat neoprávněnými osobami (řádným používáním přístupových kont, zabezpečením prostor s výpočetní technikou).
11.5. Pracovníci nesmí přistupovat do internetu rizikovým způsobem, stahovat spustitelné nebo s tím související soubory (exe, dll, ..), ani stahovat dokumenty z neověřených zdrojů.
11.6. Výše popsané soubory se nesmí ani otevírat, pokud však k této situaci dojde, je povinnost uživateli to hlásit správci IT a MBI.

12. Školení pracovníků

12.1. Všichni uživatelé aplikací ČNRDD musí být proškoleni v problematice informační bezpečnosti. Provádí se vstupní školení a dále pravidelné proškolení 1 x ročně.
12.2. Proškolení správců operačních systémů zajišťují v rámci svých postupů kybernetické bezpečnosti jednotlivé organizace (nemocnice, ZČU).

13. Hodnocení informační bezpečnosti

13.1. <u>Monitorování a hodnocení</u>
13.1.1. Dodavatel informačních technologií má definován roční plán pro posuzování informační bezpečnosti.
13.1.2. Dodavatel informačních technologií zpracovává 1x ročně zprávu *Posuzování a ošetření rizik bezpečnosti informací z hlediska informačního systému*, kterou předává MBI.
13.1.3. MBI registru sestavuje zprávu *Přezkoumání informační bezpečnosti vedením* (z hlediska informačních technologií a také z hlediska organizačního, ochrany osobních údajů atd.), která slouží jako východisko pro přezkoumání informační bezpečnosti vedením ČNRDD.
13.1.4. Zjištěné nedostatky se řeší nápravnými opatřeními, které navrhuje MBI společně se správcem informačních technologií a kontroluje DPO.
13.2. <u>Interní a externí audity</u>
13.2.1. Audit informační bezpečnosti a dodržování pravidel GDPR provádí 1 x ročně MBI registru. Součástí auditu je i audit dodavatele informačních technologií.

13.2.2. Výstup auditu předkládá ke schválení vedoucímu lékaři registru a dále k projednání na Radě kvality ČNRDD.

13.3. Analýza přístupů do aplikací

13.3.1. Hodnotí se, zda do aplikací přistupují pouze autorizované osoby, případně se aktualizuje seznam autorizovaných osob (minimálně jednou ročně).

13.3.2. Výstup analýzy se zahrnuje do *Posuzování a ošetření rizik bezpečnosti informací z hlediska informačního systému*.

13.4. Přezkoumání vedením

13.4.1. Postupy a procesy informační bezpečnosti včetně smluv s dodavateli informačních technologií musí být pravidelně ověřovány, hodnotí se jejich trvající platnost, soulad s legislativou a standardy WMDA.

13.4.2. Přezkoumání se provádí jedenkrát ročně, podklady připravuje MBI registru ve spolupráci s DPO. Jako jeden z podkladů slouží dokument *Posuzování a ošetření rizik bezpečnosti informací z hlediska informačního systému*, která obsahuje seznam incidentů, výsledky monitorování bezpečnosti a analýzu přístupu do aplikací.

13.4.3. Při přezkoumání se hodnotí:

- opatření z předchozích přezkoumání
- výsledky monitorování
- řešení incidentů
- výsledky auditů
- plnění cílů bezpečnosti
- posuzování rizik a plánů jejich ošetření

13.4.4. Zpráva z přezkoumání - *Přezkoumání informační bezpečnosti vedením*, se projednává na výroční radě kvality registru a předkládá ke schválení řediteli registru.

13.4.5. Výstupem přezkoumání jsou dle potřeby změny v systému řízení bezpečnosti informací a také příležitosti pro neustálé zlepšování.

14. Dodavatel informačních technologií

14.1. Problematika informační bezpečnosti je zakotvena ve smlouvě s dodavatelem informačních technologií, tedy ZČU.

14.2. Zajištění informační bezpečnosti musí respektovat platnou legislativu a také standardy WMDA. Činnost dodavatele se ověřuje pravidelně v rámci auditu a při přezkoumání vedením.

15. Změny a vývoj informačního systému

15.1. Podklady a požadavky ke změnám aplikací zadávají uživatelé ČNRDD a vývojový tým dodavatele informačních technologií. Všechny modifikace probíhají definovaným způsobem:

- implementace, testování a validace změn vývojovým týmem je prováděna ve vývojovém prostředí s vlastní (anonymizovanou) databází
- testování změn uživateli aplikací (testeři) je prováděna v testovacím prostředí, nedostatky se reportují vývojovému týmu
- dodavatel systému provádí před distribucí nové verze její validaci, která ověří trvající konzistentnost a funkcionalitu systému oproti předchozí verzi
- po vyřešení všech nedostatků a chyb, odsouhlasení změny a provedení validace dochází k vydání aktualizované verze aplikace do produkčního prostředí (běžného provozu)

15.2. Každá vydaná verze má unikátní pojmenování dle principů sémantického verzování.
15.3. Update provádí zhotovitel systému přímo z pracoviště na ZČU.
15.4. Dodavatel informačních technologií provozuje systém pro sledování změn všech aplikací a jejich dokumentaci.

16. Zajištění kontinuity informační bezpečnosti

16.1. V případě havárie informačního systému je stanoven postup pro obnovu činnosti a zachování dostupnosti dat. Blíže viz SOP ČNRDD/M02 *Elektronické záznamy*, kapitola *Postup při havárii*.
16.2. Informační bezpečnost musí být zajištěna i v případě mimořádných událostí, jak je definováno v SOP ČNRDD/M06 *Řešení mimořádných událostí*.
16.3. Opatření kontinuity bezpečnosti informací se pravidelně verifikují (v samotné organizaci i u správců informačních a operačních systémů), aby se ověřilo, že jsou dostatečná a efektivní.
16.4. V případě ukončení činnosti registru se všechna data předají subjektu, který bude pokračovat/naváže na činnost registru. Tento subjekt přebere zodpovědnost za data a zajištění informační bezpečnosti. Subjekt musí splňovat kvalifikační standardy WMDA a jako nástupnická organizace musí být schválen správní radou ČNRDD.
16.5. Pokud bude činnost registru ukončena kompletně bez nástupnické organizace, budou osobní data dárců a související záznamy smazány s výjimkou těch, kde byl proveden odběr krvetvorných buněk. Minimalizovaná databáze bude uložena u subjektu, který určí správní a dozorčí rada registru.
16.6. V souvislosti s ukončením činnosti registru se ukončí přístupy všech pracovníků, kteří se na dalších aktivitách registru nebudou podílet, do aplikací a databáze.

17. Dokumentace

17.1. Veškeré dokumenty dokládající plnění požadavků informační bezpečnosti musí být uchovávány minimálně po dobu 6 let.

18. Přílohy

18.1. Přezkoumání informační bezpečnosti vedením (zpracování ČNRDD).
18.2. Posuzování a ošetření rizik bezpečnosti informací z hlediska informačního systému (zpracovává ZČU).

ZMĚNY/REVIZE:

datum:	**revidoval/schválil:**	**Podpis:**	**revize/změna*:**
1.4.2021	Lysák, Houdová		implementace směrnice, vydání verze 1

* silně vyznačeny pravidelné roční revize