SLOVENSKÁ NÁRODNÁ AKREDITAČNÁ SLUŽBA

METODICKÁ SMERNICA PRE SPRÁVNU LABORATÓRNU PRAX

MSA-G/25

SPRÁVNA LABORATÓRNA PRAX A BEZPEČNOSŤ IT (OECD Guideline No. 25)

Schválil: **Ing. Štefan Král, PhD.**
riaditeľ SNAS

Účinnosť od: 28.02.2025	Vydanie: 1 Aktualizácia: 0	Označenie RD: MSA-G/25

- Tento dokument bol vytvorený elektronicky -

Táto metodická smernica je prekladom dokumentu OECD (2024), *OECD Position Paper on Good Laboratory Practice and IT Security*, OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring, No. 25, OECD Publishing, Paris..

Spracovali: **Ing. Henrieta Bóriková**
Ing. Kvetoslava Forišeková

Dátum spracovania: **10.02.2025**
Preskúmala: **RNDr. Lívia Kijovská, PhD.**

Táto MSA neprešla jazykovou úpravou.

V prípade rozdielov medzi týmto prekladom a originálom je platný text pôvodného dokumentu.

Dostupnosť MSA: https://www.snas.sk

Obsah

1 ÚVODNÉ USTANOVENIA

1.1 PREDHOVOR

Tento poradný dokument vypracovala Pracovná skupina OECD pre správnu laboratórnu prax (SLP), ktorú viedlo Dánsko (Medical Products). V prípravnej skupine boli zástupcovia Rakúska, Belgicka, Kanady, Francúzska (Medical Products), Nemecka a Švajčiarska. Dokument vychádza z publikácie o kybernetickej bezpečnosti a správnej klinickej praxi (GCP) vypracovanej na úrovni Európskej únie. Dokument preskúmala a schválila Pracovná skupina pre správnu laboratórnu prax. Za zverejnenie tohto dokumentu zodpovedá Výbor pre chemikálie a biotechnológiu, ktorý jeho zverejnenie odsúhlasil.

2 DEFINÍCIA POJMOV

Prevzaté z OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring, No.1, OECD Principles of Good Laboratory Practice (as revised in 1997).

Pozn. SNAS: Vysvetlenie špecifických pojmov je uvedené v príslušných MSA-G, ktorých sa to týka.

2.1 SLP

Zásady správnej laboratórnej praxe – systém kvality vzťahujúci sa na proces organizácie a podmienky, za ktorých sa neklinické štúdie plánujú, vykonávajú, overujú, zaznamenávajú, ukladajú a oznamujú. Neklinické štúdie sa vykonávajú na testovacích pracoviskách, ktorými sú laboratóriá, skleníky a polia.

Národný program dodržiavania zásad SLP (NP SLP) – zisťuje, či testovacie pracoviská zaviedli zásady SLP do praxe a či sú schopné zabezpečiť, že výsledné údaje majú zodpovedajúcu kvalitu. NP SLP vymedzuje pôsobnosť a rozsah programu, poskytuje informáciu o mechanizme, prostredníctvom ktorého testovacie pracovisko vstúpi do programu, o druhoch inšpekcií testovacích pracovísk a auditov štúdií, opisuje rôzne druhy inšpekcií, ako aj ich frekvenciu a vymedzuje právomoci inšpektorov.

Osvedčenie SLP – je dokument, ktorým sa deklaruje, že testovacie pracovisko (laboratórium) vykonáva štúdie (testy, skúšky) v súlade so zásadami Správnej laboratórnej praxe.

Národná monitorovacia autorita v dokumentoch OECD a EC = akreditujúca osoba (SNAS) v legislatíve SLP na Slovensku

2.2 POJMY TÝKAJÚCE SA TESTOVACIEHO PRACOVISKA

Testovacie pracovisko – pracovisko uvedené v zákone[1] vrátane osôb, priestorov a prevádzkových jednotiek potrebných na vykonávanie neklinických štúdií zdravotnej a environmentálnej bezpečnosti. Pre multicentrové štúdie, teda také, ktoré sú vykonávané na viacerých miestach, sa pod testovacím pracoviskom rozumie miesto, kde pracuje vedúci štúdie spolu so všetkými ďalšími testovacími miestami zúčastňujúcimi sa na štúdii.

Testovacie miesto – znamená také miesto, kde je vykonávaná určitá časť štúdie.

Vedenie testovacieho pracoviska – osoba(y), ktorá je zodpovedná za organizáciu a chod testovacieho pracoviska podľa zásad správnej laboratórnej praxe. Vykonáva právne úkony, administratívno-správne úkony vo všetkých veciach testovacieho pracoviska na základe zmluvy o zriadení pracoviska zakladajúcou listinou alebo zákonom.

Vedenie testovacieho miesta – (ak bolo vymenované) – osoba(y) zodpovedajúca za to, aby časť štúdie, za ktorú zodpovedá, bola vykonávaná v súlade so zásadami SLP.

Vedúci testovacieho pracoviska – v prípade zložitejšej organizačnej štruktúry testovacieho pracoviska osoba, ktorá je priamo zodpovedná za konkrétnu činnosť testovacieho pracoviska podľa zásad správnej laboratórnej praxe (riaditeľ odboru, vedúci laboratória...). Právomoci na zabezpečenie činnosti podľa zásad SLP má delegované od vedenia testovacieho pracoviska buď poverením alebo definovaním v pracovnej náplni.

Objednávateľ štúdie – subjekt, ktorý si objednáva, finančne zabezpečuje a predkladá neklinickú štúdiu zdravotnej a environmentálnej bezpečnosti na posúdenie.

(Pozri aj Nariadenie vlády č. 320/2010 Z. z. v znení neskorších predpisov, § 3, (5)).

Poznámka

Objednávateľom môže byť:

- *Subjekt*, ktorý prichádza s návrhom vykonať a podporuje, poskytnutím finančných alebo iných zdrojov, neklinické štúdie zdravotnej a environmentálnej bezpečnosti;*
- *Subjekt*, ktorý predkladá neklinické štúdie zdravotnej a environmentálnej bezpečnosti oprávnenej autorite pri registrácii produktu, alebo pri inej žiadosti, pre ktorú je súlad so zásadami SLP vyžadovaný.*

* *„Subjektom" môže byť jednotlivec, obchodná spoločnosť, združenie, vedecký, alebo akademický ústav, vládna agentúra alebo ich organizačné jednotky, alebo akýkoľvek iný právne identifikovateľný subjekt.*

Vedúci štúdie – osoba zodpovedajúca za celkové vykonanie neklinickej štúdie bezpečnosti zdravia a životného prostredia, vrátane plánu štúdie a záverečnej správy.

Vedúci čiastkovej štúdie – osoba, ktorá v prípade štúdie vykonávanej na viacerých miestach koná v mene vedúceho štúdie a zodpovedá za jemu pridelené časti štúdie.

[1] § 2 písm. e) zákona č. 67/2010 Z.z. o podmienkach uvedenia chemických látok a chemických zmesí na trh a o zmene a doplnení niektorých zákonov (chemický zákon).

Program zabezpečenia kvality (Quality Assurance Programme – QAP) – definovaný systém, zahŕňajúci zamestnancov, ktorý je nezávislý od vykonávania štúdie a slúži na zabezpečenie súladu postupu prác v testovacom pracovisku so zásadami správnej laboratórnej praxe.

Zabezpečenie kvality (Quality Assurance – QA) – zdroje zodpovedné za implementáciu a udržiavanie QAP.

Pozn.: Zodpovednosti QA v SLP, okrem iného, nezahŕňajú riadenie dokumentácie systému kvality, riadenie nástrojov pre vylepšenia organizačných procesov (hoci niektoré testovacie pracoviská môžu prideliť tieto činnosti QA), schvaľovanie odchýlok alebo schvaľovanie primeranosti zdrojov. Uznáva sa, že iné systémy kvality (napr. ISO 9000, Správna výrobná prax (GMP), ISO 17025) používajú pojem „zabezpečenie kvality" v inom kontexte.

Štandardné pracovné postupy (ŠPP) – sú dokumentované postupy, ktoré opisujú, ako vykonávať testy alebo činnosti, ktoré nie sú detailne špecifikované v študijných plánoch alebo v oficiálnych a všeobecne akceptovaných testovacích metódach (OECD, REACH).

Master Schedule – súbor informácií o vykonávaných štúdiách na testovacom pracovisku, slúži na sledovanie štúdií a vyťaženosti testovacieho pracoviska.

2.3 POJMY TÝKAJÚCE SA NEKLINICKÝCH ŠTÚDIÍ ZDRAVOTNEJ A ENVIRONMENTÁLNEJ BEZPEČNOSTI

Neklinická štúdia zdravotnej a environmentálnej bezpečnosti – ďalej len „štúdia" – znamená experiment alebo súbor experimentov, ktorými je testovaná látka skúmaná v laboratórnych podmienkach alebo v životnom prostredí, s cieľom získať údaje o jej vlastnostiach a/alebo zdravotnej a environmentálnej bezpečnosti, ktoré sú plánované ako podklad pre rozhodnutie príslušnej regulačnej autority pred jej povolením do používania.

Krátkodobá štúdia – štúdia krátkeho trvania so všeobecne používanými bežnými technikami.

Multicentrová štúdia – akákoľvek štúdia, ktorej niektoré fázy sú vykonávané na viac ako jednom mieste. Takéto štúdie sú nevyhnutné, ak je potrebné využiť miesta, ktoré sú zemepisne vzdialené, organizačne rozdielne alebo ináč oddelené. To sa týka aj oddelenia organizácie, ktoré slúži ako testovacie miesto, kým iné oddelenie tej istej organizácie pôsobí ako testovacie pracovisko.

Fáza / etapa štúdie – definovaná činnosť alebo súbor činností pri uskutočňovaní štúdie.

Plán štúdie – dokument, ktorý definuje ciele a experimentálne plánovanie skúšok na vykonávanie štúdie, vrátane jeho zmeny a doplnky.

Doplnok plánu štúdie – predstavuje cielenú zamýšľanú zmenu plánu štúdie.

Odchýlka od plánu štúdie – neočakávaná odchýlka od plánu štúdie po dátume začatia štúdie.

Testovací systém – biologický, fyzikálny alebo chemický systém alebo ich kombinácia použitá v štúdii.

Primárne údaje – všetky pôvodné záznamy a dokumentácia vypracovaná v testovacom pracovisku, alebo ich verifikované kópie, ktoré sú výsledkom pozorovaní a činností vykonaných v štúdii. Primárne údaje môžu zahŕňať aj fotografie, mikrofilmy, počítačové médiá na uchovávanie údajov, diktované pozorovania, záznamy z automatizovaných prístrojov alebo iné záznamové médiá určené na uchovávanie dát.

Vzorka – každý materiál odobratý z testovacieho systému za účelom vyšetrenia, analýzy alebo uchovávania.

Dátum začiatku štúdie – dátum, kedy vedúci štúdie podpísal plán štúdie.

Dátum experimentálneho začiatku štúdie – dátum, kedy boli získané prvé údaje zo štúdie.

Dátum ukončenia experimentu – posledný deň, kedy boli získané údaje zo štúdie.

Dátum ukončenia štúdie – dátum, kedy vedúci štúdie podpísal záverečnú správu zo štúdie.

2.4 POJMY TÝKAJÚCE SA TESTOVANEJ LÁTKY

Testovaná látka – látka, ktorá je predmetom SLP štúdie. Závery SLP štúdie poskytnú informácie o vlastnostiach testovanej látky, ktoré umožnia zhodnotiť, aké riziko predstavuje testovaná látka pre bezpečnosť ľudí, zvierat alebo pre životné prostredie.

Treba upozorniť že v niektorých OECD Test Guidelines sa pre „testovanú látku“ používa aj pojem "test chemical". (odsúhlasené v júni 2013, OECD's Joint Meeting of the Chemicals Committee and the Working Party on Chemicals, Pesticides and Biotechnology). Teda môžeme sa stretnúť aj s pojmami "test item", "test compound", "test substance". Cieľom tohto návrhu nebolo zavedenie novej definície pojmu “chemikália”, ale skôr išlo o zosúladenie terminológie s definíciou uvedenou v UN GHS pre klasifikáciu a označovanie, kde sa pod chemikáliou myslí aj “látka a zmes”

Referenčná látka – akákoľvek látka, použitá ako základ na porovnanie s testovanou látkou.

Šarža – špecifické množstvo testovanej alebo referenčnej látky vyrobené v jednom cykle výroby, takže sa dá očakávať, že majú homogénny charakter a dajú sa za také pokladať.

Nosič / Vehikulum – akákoľvek látka, ktorá slúži ako nosič na zmiešavanie, dispergovanie, alebo zvyšovanie rozpustnosti testovanej a/alebo referenčnej látky s cieľom umožnenia a zjednodušenia jej podávania/aplikácie testovaciemu systému.

Formulácia (test. látka + nosič) – kombinácia testovanej látky a rôznych prísad, ako pomocných látok, ktoré sú skombinované a podávané a/alebo aplikované testovaciemu systému v rôznych formách (napr. tabletky, kapsule, roztok...).

Príprava testovanej látky/alebo pripravená testovaná látka – môže byť formuláciou (alebo zmesou) obsahujúcou testovanú látku, alebo testovanú látku v nosiči, kde sa táto kombinácia získa riedením, miešaním, dispergovaním, vytvorením suspenzie, rozpustením a/alebo iným procesom so zámerom aplikovať ju testovaciemu systému. Testovaciemu pracovisku môže byť dodaná testovaná látka (na priame podanie), alebo testovaná látka, ktorá ešte musí byť nejako pripravená alebo prípravok s testovanou

látkou, ktorý možno priamo podať alebo aplikovať testovaciemu systému (tiež nazývaná "ready-to-use").

Testovaná látka, ktorá je zapuzdrená (encapsulated) alebo balená iným spôsobom, bez prítomnosti pomocných látok alebo nosiča, sa nepovažuje za to isté ako „pripravená testovaná látka" opisovaná v tomto dokumente.

Charakterizácia – určuje vlastnosti testovanej látky a poskytuje dôkazy na podporu vhodnosti jej použitia v SLP štúdiách.

Identifikácia – proces kontroly a hodnotenia testovanej látky porovnaním s dodanými informáciami, s cieľom určiť, či testovaná látka je tá, ako bola očakávaná. Poskytnutými informáciami môžu byť prepravné doklady, e-maily od dodávateľa, označenie etiketou na testovanej látke, atď. Typickými znakmi používanými na identifikáciu testovanej látky môžu byť – názov, číslo šarže, čistota, koncentrácia, zloženie, chemické, fyzikálne a biologické parametre. Identifikácia môže tiež zahŕňať fyzikálnu a/alebo analytickú kontrolu. Proces identifikácie musí byť vykonaný pred začiatkom experimentálnej fázy SLP štúdie.

Dátum exspirácie – stanovený dátum, do ktorého sa očakáva, že testovaná látka si zachová svoje vlastnosti v rámci špecifikácií, pokiaľ je skladovaná za definovaných podmienok a po uplynutí ktorého už nemôže byť použitá.

Dátum retestovania – dátum, kedy testovaná látka môže byť znovu otestovaná, s cieľom ubezpečiť sa, že je ešte stále vhodná na použitie.

2.5 POJMY TÝKAJÚCE SA INŠPEKCIE TESTOVACIEHO PRACOVISKA

Inšpekcia testovacieho pracoviska – kontrola postupov testovacieho pracoviska a praktických činností smerujúcich k dosiahnutiu stupňa zhody so zásadami SLP, počas ktorej sa skontrolujú systémy riadenia a pracovné postupy testovacieho pracoviska, ako aj integrita údajov, aby sa zabezpečilo, že výsledné údaje majú náležitú kvalitu na posúdenie a rozhodovanie národnými regulačnými orgánmi.

Inšpektor – osoba, vykonávajúca inšpekcie testovacích pracovísk a audity neklinických štúdií v zastúpení akreditujúcej osoby (SNAS).

Audit štúdií – porovnanie prvotných údajov a súvisiacich záznamov v predbežnej alebo záverečnej správe, s cieľom určiť, či primárne údaje boli presne zaznamenané, či sa testovanie vykonalo v súlade s plánom štúdie a štandardnými pracovnými postupmi, získať dodatočné informácie neuvedené v správe a stanoviť, či postupy použité pri spracovaní údajov mohli ovplyvniť ich validitu.

Správa o inšpekcii – oficiálny písomný doklad o vykonanej inšpekcii, v ktorej sú identifikované všetky posudzované prvky a činnosti, menovite uvedené všetky nedostatky a posúdená miera dodržiavania zásad SLP. Určuje kvalitu a integritu údajov preverovaného testovacieho pracoviska.

3 SKRATKY

GLP	Good Laboratory Practice
MSA	Metodická smernica
OECD	Organizácia pre hospodársku spoluprácu a rozvoj (Organisation for Economic Cooperation and Development)
SLP	Správna laboratórna prax
SNAS	Slovenská národná akreditačná služba
ŠPP	Štandardný pracovný postup
SR	Slovenská republika
ÚZK/QAU	Útvar zabezpečenia kvality/Quality Assurance Unit
NP SLP	Národný program dodržiavania zásad SLP
TFM	Vedenie testovacieho pracoviska (Test Facility Management)
QA	Pracovník ÚZK (Quality Assurance)
QAP	Program zabezpečenia kvality (Quality Assurance Programme)
REACH	Európska chemická legislatíva – REACH (Registration, Evaluation, Authorisation of Chemicals)

4 SÚVISIACE PREDPISY

Zákon 67/2010 Z. z. o podmienkach uvedenia chemických látok a chemických zmesí na trh a o zmene a doplnení niektorých zákonov (chemický zákon)

Nariadenie vlády č. 320/2010 Z. z., ktorým sa upravujú činnosti testovacích pracovísk a činnosti inšpektorov vykonávajúcich inšpekcie, audit a overovanie dodržiavania zásad správnej laboratórnej praxe.

Nariadenie vlády SR č. 92/2012 Z. z., ktorým sa mení a dopĺňa nariadenie vlády Slovenskej republiky č. 320/2010 Z. z., ktorým sa upravujú činnosti testovacích pracovísk a činnosti inšpektorov vykonávajúcich inšpekcie, audit a overovanie dodržiavania zásad správnej laboratórnej praxe**.**

Zákon č. 53/2023 Z. z. o akreditácii orgánov posudzovania zhody

MSA série G – všetky MSA vydané SNAS, týkajúce sa SLP dostupné na webovej stránke www.snas.sk

EU

Smernica 2004/9/ES o inšpekcii a overovaní správnej laboratórnej praxe (kodifikovaná verzia)

Smernica 2004/10/ES o zosúlaďovaní zákonov, predpisov a správnych opatrení uplatňovaných na zásady správnej laboratórnej praxe a overovanie ich uplatňovania pri testoch chemických látok (kodifikovaná verzia)

Nariadenie Európskeho parlamentu a Rady (ES) č. 1907/2006 z 18. decembra 2006 o registrácii, hodnotení, autorizácii a obmedzovaní chemikálií **(REACH)** a o zriadení európskej chemickej agentúry (ECHA), o zmene a doplnení smernice 1999/45/ES

a o zrušení nariadenia Rady (EHS) č. 793/93 a nariadenia Komisie (ES) č. 1488/94, smernice rady76/769/EHS a smerníc Komisie 91/155/EHS, 93/67/EHS, 93/105/ES a 2000/21/ES, v platnom znení.

Nariadenie Európskeho parlamentu a Rady (ES) č. 1272/2008 zo 16. decembra 2008 o klasifikácii, označovaní a balení látok a zmesí, o zmene, doplnení a zrušení smerníc 67/548/EHS a 1999/45/ES a o zmene a doplnení nariadenia (ES) č. 1907/2006, platnom znení.

Nariadenie Komisie č. 440/2008 z 30. mája 2008, ktorým sa ustanovujú testovacie metódy podľa nariadenia EP a R č. 1907/2006 o registrácii, hodnotení, autorizácii a obmedzovaní chemických látok **(REACH)**.

OECD

1981 Council Act Decision [C (81)30/Final] on the Mutual Acceptance of Data in the Assessment of Chemicals,

1989 Council Decision Recommendation on Compliance with Principles of Good Laboratory Practice [C (89)87/Final]

5 VECNÁ ČASŤ

5.1 ÚVOD

Údaje SLP sa čoraz viac vytvárajú a uchovávajú v elektronickej podobe. Cieľom opatrení bezpečnosti IT je chrániť elektronické SLP údaje a aplikácie pred špecifickými rizikami, ktoré sa vyskytujú v počítačovom prostredí.

Hrozby a útoky na systémy obsahujúce SLP údaje a zodpovedajúce opatrenia na zaistenie bezpečnosti takýchto systémov sa neustále vyvíjajú, najmä v prípade systémov a služieb poskytovaných prostredníctvom internetu alebo s ním prepojených.

Testovacie pracoviská môžu zveriť riešenie bezpečnosti IT externým poskytovateľom služieb. Zodpovednosť však zostáva na testovacom pracovisku. Odporúčania a rady dodávateľov operačných systémov a platforiem by sa mali starostlivo zvážiť a v prípade potreby uplatniť.

5.2 ROZSAH PÔSOBNOSTI

Tento poradný dokument sa týka elektronických SLP údajov a prepojených počítačových systémov umiestnených na serveroch, ktoré môžu byť vystavené počítačovým narušeniam.

Pozn. SNAS: Teda ich zneužitiu a nezákonnej manipulácii s údajmi.

Pojmy uvedené v tomto dokumente pre "testovacie pracovisko", "vedenie testovacieho pracoviska" a "vedúcich štúdií" sa rovnako sa vzťahujú na "testovacie miesta", "vedenie testovacieho miesta" a "vedúceho čiastkovej štúdie", ak sa delegované fázy štúdie

vykonávajú ako súčasť multicentrovej štúdie (tieto pojmy sú definované v zásadách SLP).

5.3 PRIEBEŽNÉ BEZPEČNOSTNÉ OPATRENIA A ZODPOVEDNOSTI V RÁMCI SLP

Vedenie testovacieho pracoviska musí udržiavať bezpečnostný systém, ktorý zabraňuje neoprávnenému prístupu a zabezpečuje dostupnosť SLP údajov. Postupy a opatrenia na zaistenie bezpečnosti IT by mali byť založené na riziku a dôsledkoch porúch systému alebo interných či externých úmyselných alebo neúmyselných zásahoch, ktoré by mohli nepriaznivo ovplyvniť integritu SLP údajov.

5.4 FYZICKÁ BEZPEČNOSŤ

Servery, počítače, infraštruktúra a médiá, na ktorých sú uložené SLP údaje a počítačové systémy relevantné pre SLP, musia byť fyzicky chránené pred neoprávneným prístupom, poškodením a stratou. Rozsah bezpečnostných opatrení závisí od kritickosti údajov.

Vedenie testovacieho pracoviska musí zabezpečiť primeranú úroveň zabezpečenia dátových centier, ako aj lokálneho hardvéru, ako sú servery, počítače, tablety, telefóny, pevné disky a USB disky.

V dátových centrách, v ktorých sa nachádzajú SLP údaje a aplikácie, sa musí fyzický prístup obmedziť len na nevyhnutné minimum. Je možné použiť dvojfaktorovú autentifikáciu. Dátové centrá musia byť konštruované tak, aby sa minimalizovalo riziko a vplyv prírodných katastrof, musí byť zabezpečená kontrola škodcov a účinné opatrenia proti požiaru (napr. chladenie, detekcia ohňa a hasenie požiaru), záplavám a akýmkoľvek iným príčinám, ktoré by mohli zmeniť resp. poškodiť údaje. Zvyčajne sú k dispozícii núdzové generátory a neprerušiteľné zdroje napájania (UPS) spolu s redundantnými poskytovateľmi internetového protokolu. V prípade, že je dátové centrum typu ´co-location´, servery musia byť uzamknuté a fyzicky chránené (napr. v klietkach), aby sa zabránilo prístupu iných používateľov (´co-location´ - spoločné umiestnenie, znamená dátové centrá, kde hostovaný hardvér patrí viacerým organizáciám, ktoré majú prístup do serverových miestností).

Údaje sa prednostne majú replikovať v primeranej frekvencii z primárneho dátového centra do sekundárneho záložného miesta, ktoré je dostatočne fyzicky vzdialené, aby sa minimalizovalo riziko, že rovnaký požiar alebo prírodná katastrofa zničí obe dátové centrá. Musí byť zavedený a testovaný plán obnovy po havárii.

5.5 FIREWALLY

Na zabezpečenie bariéry medzi dôveryhodnou internou sieťou a nedôveryhodnou externou sieťou, ako aj na kontrolu prichádzajúcej a odchádzajúcej sieťovej prevádzky (z určitých IP adries, cieľových miest, protokolov, aplikácií alebo portov atď.) je potrebné zaviesť účinné firewally. Pravidlá brány firewall musia byť definované tak prísne, ako je to prakticky možné, a musia umožňovať len nevyhnutnú a povolenú komunikáciu.

Keďže pravidlá brány firewall sa časom menia alebo sa stávajú nedostatočnými (napr. preto, že dodávatelia softvéru a technici IT potrebujú otvoriť určité porty z dôvodu inštalácie alebo údržby aplikácií, prípadne v dôsledku vývoja kybernetických hrozieb), pravidelne sa revidujú. Táto kontrola musí zabezpečiť, že aktuálne pravidlá brány firewall sú stále nastavené čo najprísnejšie.

Pozn. SNAS: Firewall je hardvérové/softvérové riešenie, ktoré umožňuje izolovať počítačové siete organizácie, čím ich chráni pred vonkajším ohrozením.

5.6 MANAŽMENT ZRANITEĽNÝCH MIEST

Kritické zraniteľné miesta operačných systémov a platforiem možno zneužiť na to, aby neoprávnené osoby získali privilegovaný prístup k systémom, upravili alebo vymazali údaje a znemožnili legitímnym používateľom prístup k nim. Takéto zneužitia sa vyskytujú v operačných systémoch pre servery, počítače, tablety, mobilné telefóny a routery, ako aj v platformách pre databázy atď. Kým sú tieto operačné systémy a platformy podporované, výrobcovia pravidelne vydávajú bezpečnostné záplaty (opravy) na odstránenie týchto zraniteľných miest. Preto je nevyhnutné včas aplikovať príslušné kritické bezpečnostné záplaty pre platformy a operačné systémy (odporúča sa okamžite).

Systémy, ktoré nie sú včas bezpečnostne opravené, predstavujú veľké riziko straty integrity údajov. V prípade potreby musia byť takéto systémy izolované od počítačových sietí a internetu.

5.7 MANAŽMENT PLATFORIEM

Operačné systémy a platformy pre kritické aplikácie a komponenty sa musia aktualizovať včas, aby sa zabránilo ich používaniu v nepodporovanom stave.

Nepodporované platformy a operačné systémy, pre ktoré nie sú k dispozícii bezpečnostné záplaty, sú vystavené vyššiemu riziku zraniteľnosti. Validácia aplikácií na nových operačných systémoch a platformách a migrácia údajov sa musí plánovať vopred a včas dokončiť.

Nepodporované platformy a operačné systémy musia byť izolované od počítačových sietí a internetu.

5.8 OBOJSMERNÉ ZARIADENIA (napr. USB)

Obojsmerné zariadenia (napr. USB) alebo iné prenosné médiá alebo zariadenia, ktoré môžu byť používané aj mimo testovacieho pracoviska, by mohli ohroziť systém. Z tohto dôvodu sa musia prísne kontrolovať, pretože môžu úmyselne alebo neúmyselne vniesť škodlivý softvér a ovplyvniť integritu a dostupnosť údajov.

5.9 ANTIVÍRUSOVÝ SOFTVÉR

V systémoch používaných v SLP musí byť nainštalovaný a aktivovaný antivírusový softvér. Antivírusový softvér musí byť neustále aktualizovaný najnovšími definíciami vírusov s cieľom identifikovať, umiestniť do karantény a odstrániť známe počítačové vírusy. Tento proces sa musí monitorovať.

5.10 TESTOVANIE PRIENIKU

V prípade systémov, ktoré sú pripojené na internet, sa musí v pravidelných intervaloch vykonávať testovanie prieniku s cieľom vyhodnotiť primeranosť prijatých bezpečnostných opatrení a identifikovať slabé miesta v zabezpečení systému, vrátane možnosti neoprávnených strán získať prístup k systému a jeho údajom a kontrolovať ich. Zistené zraniteľné miesta, najmä tie, ktoré súvisia s potenciálnou stratou integrity údajov, sa musia včas riešiť a zmierňovať.

5.11 DETEKCIA A PREVENCIA PRIENIKOV

V systémoch, ktoré sú pripojené na internet, sa musí zaviesť účinný systém detekcie a prevencie vniknutí, aby bolo možné monitorovať sieť z hľadiska pokusov o vniknutie z externých strán a navrhovať a udržiavať účinné preventívne opatrenia.

Hrozby prostredníctvom bezdrôtových pripojení sa musia považovať za rizikové a môžu si vyžadovať podobný prístup.

5.12 MONITOROVANIE INTERNÝCH ČINNOSTÍ

Musí byť zavedený, v rozsahu danom vnútroštátnymi pracovnoprávnymi predpismi, účinný systém na zisťovanie neobvyklých alebo rizikových činností používateľov (napr. zmena v štruktúre činností).

5.13 MANAŽMENT BEZPEČNOSTNÝCH INCIDENTOV

Testovacie pracoviská musia pracovať podľa postupu, ktorý definuje a dokumentuje bezpečnostné incidenty. Takéto incidenty sa musia riešiť z hľadiska kritickosti a kde

je potrebné, zaviesť účinné nápravné a preventívne opatrenia na zabránenie ich opakovania. V prípadoch, keď došlo alebo mohlo dôjsť k ohrozeniu údajov, postupy musia zahŕňať požiadavky na nahlásenie bezpečnostných incidentov príslušným stranám. Pri využívaní poskytovateľa služieb dohoda o úrovni služieb musí zabezpečiť, že incidenty budú včas postúpené vedeniu testovacieho pracoviska, aby vedenie testovacieho pracoviska mohlo nahlásiť závažné porušenia všetkým relevantným stranám (vedúcim štúdií, objednávateľom štúdií, archivárovi...).

5.14 METÓDA OVEROVANIA

Metóda overovania (autentifikácie) v systémoch musí identifikovať používateľov s vysokou mierou istoty. Minimálna prijateľná metóda je prostredníctvom identifikácie používateľa a hesla. Potreba prísnejších metód overovania sa musí určiť na základe posúdenia rizika, kritickosti údajov a môže zaviesť aj ďalšie metódy overovania, ako napríklad dvojfaktorové overovanie.

Dvojfaktorové overovanie predpokladá použitie dvoch z nasledujúcich troch faktorov:

- niečo, čo viete, napr. identifikáciu používateľa a heslo.
- niečo, čo máte, napr. bezpečnostný token, certifikát alebo mobilný telefón a prístupový kód SMS.
- niečo, čo ste, napr. odtlačok prsta alebo skener dúhovky (biometria).

Používateľské účty sa automaticky zablokujú po vopred definovanom počte neúspešných pokusov o overenie, a to buď na definovaný čas, alebo až kým ich správca systému po príslušných bezpečnostných kontrolách znovu neaktivuje.

5.15 VZDIALENÉ OVEROVANIE

Vzdialený prístup k SLP údajom a aplikáciám, napr. ku cloudovým systémom, prináša špecifické výzvy. Úroveň zabezpečenia musí byť primeraná kritickosti údajov (napr. údaje potrebné na rekonštrukciu štúdií SLP) a prístupovým právam, ktoré sú udelené (práva len na čítanie, zápis, alebo dokonca práva "administrátora"). Na vymedzenie typu požadovanej kontroly prístupu sa musí použiť prístup založený na riziku v závislosti od úrovne rizika.

5.16 ZÁSADY POUŽÍVANIA HESIEL

Musia sa zaviesť postupy pre pravidlá používania hesiel. Pravidlá musia zahŕňať okrem iného dĺžku, zložitosť, dobu platnosti hesla, pokusy o prihlásenie a resetovanie odhlásenia.

Pravidlá musia byť vyžadované systémami, overované počas validácie systému,

zahrnuté do pravidelných revízií validácie systému a osobitne riešené po zistení prieniku. Cieľom pravidiel pre heslá je zabrániť narušeniu.

5.17 DÔVERNOSŤ HESLA

Heslá musia byť dôverné. Heslá, ktoré používateľ pôvodne dostal zo systému alebo od manažéra, či správcu systému, musí zmeniť pri prvom pripojení k systému. Toto musí byť systémom požadované.

5.18 ODHLÁSENIE V PRÍPADE NEČINNOSTI

Možno zvážiť použitie systémov, zahŕňajúcich automatickú nečinnosť, ktoré používateľa po definovanom čase nečinnosti odhlásia. V takom prípade by používateľ nemal mať možnosť nastaviť čas odhlásenia pri nečinnosti (mimo vymedzených a prijateľných hraníc) alebo deaktivovať túto funkciu. Po odhlásení z nečinnosti sa vyžaduje úplné opätovné overovanie (napr. zadanie hesla).

5.19 VZDIALENÉ PRIPOJENIE

Pri vzdialenom pripojení k systémom cez internet sa musí používať bezpečný a šifrovaný protokol (virtuálna súkromná sieť (VPN - virtual private network) a/alebo bezpečný hypertextový prenosový protokol (HTTPS - hypertext transfer protocol secure)).

5.20 OCHRANA PROTI NEOPRÁVNENÝM ZMENÁM NA BACK-ENDE

Integrita údajov musí byť chránená proti neoprávneným zmenám vykonaným na strane servera (back-end) priamo v databáze správcom databázy. Metódou na zabránenie takýmto zmenám by mohlo byť nastavenie aplikácie tak, aby šifrovala svoje údaje v databáze, alebo uloženie nešifrovaných údajov so šifrovanou kópiou. V oboch prípadoch nemôže byť správca databázy totožný so správcom aplikácie.

5.21 ZÁLOHOVANIE

Zálohy sa vytvárajú, uchovávajú a ukladajú podľa stanovených postupov, aby sa zabezpečilo, že SLP údaje možno obnoviť v prípade, ak boli náhodne alebo úmyselne zmenené alebo vymazané, stratené v dôsledku poruchy hardvéru alebo poškodené, napr. v dôsledku kybernetického útoku. Frekvencia, uchovávanie a bezpečné skladovanie záloh je kriticky dôležité pre účinnosť procesu na zmiernenie týchto incidentov. Zálohovanie sa vykonáva vo vhodných intervaloch (napr. hodinových, denných, týždenných a mesačných) a ich uchovávanie (napr. týždeň, mesiac, štvrťrok,

navždy) sa musí určiť na základe prístupu založeného na rizikách. Zálohy sa neukladajú na tom istom fyzickom mieste, v tej istej logickej sieti alebo za tým istým firewallom ako pôvodné údaje, aby sa zabránilo ich súčasnému zničeniu alebo zmene.

V závislosti od požiadaviek na rýchlu obnovu po havárii môže byť potrebné zálohovať aj aplikácie a systémové konfigurácie, pretože inak by obnovenie služieb mohlo trvať dlho.

Obnovenie údajov a prípadne aplikácií a konfigurácií zo zálohy sa musí testovať.

5.22 ŠTANDARDNÉ PRACOVNÉ POSTUPY (SOP)

Musia byť zavedené postupy/politiky opisujúce, aké bezpečnostné opatrenia pre IT testovacie pracovisko zaviedlo a prijalo. Musí sa tiež jasne opísať, ako bude pracovisko postupovať pri akomkoľvek narušení bezpečnosti IT a pracovisko musí upozorniť svoj národný monitorovací orgán pre dodržiavanie SLP v prípade akýchkoľvek problémov s bezpečnosťou IT a straty/krádeži údajov.

***