SLOVENSKÁ NÁRODNÁ AKREDITAČNÁ SLUŽBA

METODICKÁ SMERNICA PRE SPRÁVNU LABORATÓRNU PRAX

MSA-G/17

APLIKÁCIA ZÁSAD SLP NA POČÍTAČOVÉ SYSTÉMY (OECD Guideline No. 17)

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

Účinnosť od: 30.11.2024	Vydanie: 2 Aktualizácia: 0	Označenie RD: MSA-G/17

- Tento dokument bol vytvorený elektronicky -

Slovenská národná akreditačná služba, Karloveská 63, P.O.BOX 74, 840 00 Bratislava
Tel.: +421/948 349 517
E-mail: snas@snas.sk
Internetová adresa:
www.snas.sk
IČO: 30809673
DIČ: 2020815115
IČ DPH: SK2020815115
Bankové spojenie:
BIC/SWIFT: SPSRSKBAXXX
IBAN: SK02 8180 0000 0070 0036 9571

Táto metodická smernica je prekladom dokumentu OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring, No. 17,
Application of GLP Principles to Computerised Systems.
ENV/JM/Mono(2016)13

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

Dátum spracovania: **05.11.2024**

Preskúmala: **RNDr. Lívia Kijovská, PhD.**

Nadobudnutím účinnosti tejto MSA končí účinnosť **MSA-G/17** zo dňa 01.09.2017.

Táto MSA neprešla jazykovou úpravou.

Dostupnosť MSA: https://www.snas.sk

Obsah

1 ÚVODNÉ USTANOVENIA

1.1 PREDHOVOR

Na svojom 26. zasadaní v roku 2012 pracovná skupina OECD pre Správnu laboratórnu prax zriadila návrhovú komisiu pod vedením Rakúskeho federálneho úradu pre bezpečnosť v zdravotníctve (Rd. Ronald BAUER) za účelom aktualizovania OECD GLP Guideline č. 10 z roku 1995 – Aplikácia zásad SLP na počítačové systémy. Návrhová komisia sa skladala zo zástupcov z Rakúska, Belgicka, Írska, Talianska, Švajčiarska, Spojeného kráľovstva a EPA zo Spojených štátov.

Tento dokument nahrádza konsenzný dokument z roku 1995. Ponecháva celý kľúčový text z dokumentu č. 10 z roku 1995, ale zahŕňa aj nový text, odrážajúci aktuálny stav v tejto oblasti. Tento návrh Poradného dokumentu bol zverejnený na verejne dostupnej webovej stránke pre SLP dňa 17. septembra 2014 a verejnosť bola vyzvaná, aby predložili svoje pripomienky do 14. novembra 2014. V tomto dokumente sú už tieto pripomienky zapracované. V roku 2022 bol tento dokument revidovaný a vydaný s doplnenou poznámkou pod čiarou na strane 11.

Tento dokument je publikovaný OECD a zodpovedá zaň Joint Meeting of the Chemicals Committee a the Working Party on Chemicals, Pesticides and Biotechnology, OECD.

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

1. Tento dokument zavádza prístup k validácii a prevádzke počítačových systémov cez ich životný cyklus. Kladie dôraz na hodnotenie rizika ako ústredného prvku merateľného, hospodárneho a efektívneho procesu validácie, so zameraním na integritu údajov. Cieľom tohto dokumentu je poskytnúť návod, ktorý umožní testovacím pracoviskám vypracovať adekvátnu stratégiu pre validáciu a prevádzku akéhokoľvek typu počítačového systému (bez ohľadu na jeho komplexnosť) v prostredí SLP.

5.1.1 Rozsah a definícia pojmov

2. Príslušné pojmy sú definované v Slovníku významov v Prílohe 2.

5.1.1.1. Počítačový systém

3. Táto smernica sa vzťahuje na všetky typy počítačových systémov používaných pri regulovaných činnostiach vyžadujúcich SLP, bez ohľadu na ich komplexnosť (od jednoduchých zariadení, ako sú váhy, až po komplexnejšie zariadenia, ako sú samostatné počítače riadiace laboratórne prístroje a komplexné systémy, ako LIMS). Počítačový systém pozostáva z hardvéru, softvéru a prepojení s jeho operačným prostredím. Hardvér pozostáva z fyzických komponentov počítačového systému; zahŕňa počítačovú jednotku ako takú a jej periférne komponenty. Softvér je program, alebo programy, ktoré riadia prevádzku počítačového systému. Všetky zásady SLP, ktoré sa vzťahujú na zariadenia, sa preto vzťahujú ako na hardvér, tak aj na softvér. Pri plánovaní, vykonávaní, oznamovaní a archivovaní štúdií môže byť používaných viac počítačových systémov na rôzne účely. K týmto účelom môže patriť priamy alebo nepriamy zber údajov z automatizovaných prístrojov, prevádzka/riadenie automatických zariadení a spracovávanie, oznamovanie

a uchovávanie údajov. Preto musia byť zavedené vhodné postupy na kontrolu, udržiavanie a prevádzkovanie počítačových systémov.

5.1.1.2. Validácia

4. Preukázanie toho, že počítačový systém je v priebehu celého svojho životného cyklu vhodný pre určené zámery, má zásadný význam a označuje sa ako validácia počítačového systému. Všetky počítačové systémy používané na generovanie, meranie, výpočet, hodnotenie, prenos, spracovanie, uchovávanie alebo archivovanie údajov určených na regulačné podanie, alebo na podporu regulačných rozhodnutí, musia byť validované, prevádzkované a udržiavané spôsobom, ktorý je v súlade so zásadami SLP.

Pozn. SNAS: ***Regulačné podanie (dosier)****: Údaje a dokumenty, ktoré sa predkladajú regulačným orgánom, aby schválili alebo monitorovali produkty, ako sú lieky, potraviny, chemikálie, atď.*

Rovnaké požiadavky sa vzťahujú aj na počítačové systémy, používané na tvorbu iných, pre SLP relevantných údajov, ako sú záznamy primárnych údajov, podmienok prostredia, záznamy o zamestnancoch a školeniach, dokumentácia o údržbe, atď. Proces, ktorý daný počítačový systém vykonáva, musí byť spoľahlivý a primeraný danému účelu. Proces validácie musí poskytnúť vysoký stupeň záruky, že počítačový systém spĺňa vopred určené špecifikácie. Validácia musí byť vykonaná na základe oficiálneho plánu validácie a to pred spustením počítačového systému do prevádzky.

5. Validácia novozavedených počítačových systémov musí byť robená vopred. V závislosti na veľkosti, kritickosti a inovatívnosti počítačového systému by testovanie malo byť, pokiaľ je to možné, vykonané vo vyhradenom validovacom prostredí predtým, ako je počítačový systém prenesený do laboratória. Pri príslušných simuláciách musí byť zabezpečené, že validovacie prostredie je rovnocenné s prostredím laboratória. Počas celého životného cyklu systému, vrátane jeho vyradenia, musí byť robená primeraná kontrola zmien.

6. Retrospektívna validácia nie je povolená, s výnimkou prípadov, kedy sa zmenil rozsah použitia, alebo sa existujúci systém stal relevantným pre SLP (napr. potreba súladu so zásadami SLP nebola predvídaná alebo špecifikovaná). Pokiaľ dôjde k takejto situácii, potom musí byť vopred dokumentovane zdôvodnené použitie daného systému v SLP štúdii. Toto zdôvodnenie musí zahŕňať retrospektívne hodnotenie vhodnosti, ktoré začína zhromaždením relevantných záznamov z minulosti, týkajúcich sa počítačového systému. Tieto záznamy musia byť preskúmané a musí byť vypracované písomné zhrnutie. Toto retrospektívne zhrnutie musí špecifikovať, aký dôkaz je k dispozícii a aké dodatočné požiadavky musia byť otestované v priebehu formálneho akceptačného testovania, aby bol dosiahnutý status validovaného systému.

5.1.1.3. Kvalifikácia

7. Pre komerčné systémy /Commercial Off-The-Shelf (COTS)/, jednoduché automatizované systémy, alebo malé systémy, je skôr akceptovaná formálna kvalifikácia ako validácia. Z dôvodu ich rozšíreného používania, sa zabudovaný softvér pokladá za validovaný v prípadoch, kedy v systéme nie je vykonávané žiadne ďalšie prispôsobenie potrebám laboratória. Ďalšie informácie možno nájsť v príslušnej smernici z oblasti Správnej výrobnej praxe (SVP), ako napr. v Prílohe č.15, Smernice EU pre Správnu

výrobnú prax pre medicínske výrobky pre použitie u ľudí a veterinárne použitie, týkajúcej sa „Kvalifikácie a validácie“.

8. Ako príklady jednoduchých komerčne vyrábaných systémov, automatizovaných zariadení alebo malých systémov možno uviesť: analytické zariadenia, ako sú napr. elektronické pipety, váhy, fotometre a zariadenia na uskladňovanie, ako sú chladničky, mrazničky, atď.

9. Vedenie testovacieho pracoviska musí rozhodnúť a definovať kritériá, kedy použiť pre počítačový systém validáciu a/alebo kvalifikáciu. Pri definovaní kritických parametrov procesu a činností slúžiacich na monitorovanie každého procesu, aby bolo zabezpečené, že tento bude kontrolovaný počas celej životnosti počítačového systému, musí byť použitý prístup založený na manažmente rizika. Preto sa očakáva, že budú zavedené prísne opatrenia pre kalibráciu a údržbu, v kombinácii s dodržiavaním interných predpisov alebo noriem, s presnými, vopred definovanými špecifikáciami. Pri kontrole procesov (napr. kontrolné grafy) sa odporúča aplikácia štatistických nástrojov a očakáva sa dlhodobá spätná vysledovateľnosť výsledkov monitorovania. Tam, kde dochádza k prepojeniu s inými systémami, je potrebné venovať špeciálnu pozornosť monitorovaniu a kontrole toku údajov. Musia byť zavedené štandardné postupy, jasne opisujúce definovaný proces a jednotlivé kroky kontroly.

10. Opakovaná kvalifikácia musí byť vykonávaná na základe vopred určených časových intervalov, berúc do úvahy identifikované riziká. Postupy pri kvalifikácii musia byť podrobne opísané.

11. Pokiaľ sa v testovacom pracovisku používa viac kusov toho istého zariadenia, môžu byť ako referencie uvedené existujúce plány a správy z už vykonanej kvalifikácie takéhoto zariadenia.

5.1.1.4. Životný cyklus

12. Prístup k validácii musí byť založený na hodnotení rizika a manažment testovacieho pracoviska sa môže slobodne rozhodnúť, aký vhodný model životného cyklu bude používať. Tento musí zabezpečiť, že činnosti súvisiace s validáciou budú definované a vykonávané systematicky a to od vypracovania koncepcie, porozumenia požiadavkám, cez vývoj, uvoľnenie, použitie v prevádzke až po vyradenie systému. Všetky relevantné fázy životného cyklu musia byť dokumentované a definované. Týkať sa to môže zakúpenia, špecifikácie, návrhu, vývoja a testovania, zavedenia do používania, prevádzky a vyradenia počítačového systému. Činnosti v rámci životného cyklu musia byť odstupňované na základe dokumentovaného hodnotenia rizík. Pre jednoduché postupy, ako napríklad váženie na samostatných váhach, je možné vyžadovať len minimum činností; pre komplexné systémy, ako napríklad navzájom prepojené systémy riadenia laboratórnych informácií (LIMS), môžu byť vyžadované rozsiahlejšie činnosti.

5.1.2 Riadenie rizík

13. V priebehu celého životného cyklu počítačového systému musí byť zavedené riadenie rizík, berúce do úvahy potrebu zabezpečiť integritu údajov a kvalitu výsledkov

štúdie. Riadenie rizík pozostáva z identifikácie rizika, hodnotenia rizika, zníženia rizika a kontroly rizika. Rozhodnutie o rozsahu validácie a kontroly integrity údajov, musí byť založené na zdokumentovanom logickom odôvodnení a dokumentovanom hodnotení rizík. Riadenie rizík musí byť prepojené s inými relevantnými postupmi (napr. riadenie konfigurácie a zmeny, riadenie postupov pre údaje, obchodné riziko, atď.).

14. Pri vypracovávaní adekvátnej stratégie validácie a pri odstupňovaní rozsahu validácie podľa závažnosti, musí byť používané hodnotenie rizík. Vykonanie validácie musí byť motivované zamýšľaným použitím systému a potenciálnym rizikom na kvalitu a integritu údajov. Výstup z procesu hodnotenia rizika musí vyústiť do plánu primeraných činností validácie celých počítačových systémov, alebo jednotlivých funkcionalít počítačového systému. Primerané využitie metódy hodnotenia rizika je kľúčovým pre efektívnu validáciu. Pokiaľ sú výstupy z hodnotenia rizika použité správne, potom vedeniu testovacieho pracoviska poskytnú metodológiu, vhodnú na validáciu ako jednoduchých laboratórnych systémov, tak aj zložitých systémov riadenia laboratórnych údajov (LIMS).

15. Hodnotenie rizika počítačových systémov ktoré sú využívané pre SLP a aj pre štúdie mimo-SLP, musí zahŕňať akýkoľvek potenciálny vplyv činností vykonávaných mimo SLP na činnosti, ktoré musia byť vykonané v súlade so zásadami SLP. Na tieto systémy sa vzťahujú rovnaké požiadavky na validáciu, ako pri počítačových systémoch, ktoré sa využívajú výlučne na SLP štúdie. SLP údaje musia byť jasne odlíšené od údajov, ktoré nie sú získané v súlade s požiadavkami zásad SLP.

5.1.3 Zamestnanci, úlohy a zodpovednosti

16. Zásady SLP vyžadujú, aby testovacie pracovisko alebo testovacie miesto malo primerane kvalifikovaných a skúsených zamestnancov a aby boli zdokumentované školiace programy, špecifické pre jednotlivé úlohy, vrátane školení priamo na pracovisku a tam, kde je to vhodné, aj účasti na externých školiacich kurzoch. Záznamy o takýchto školeniach musia byť udržiavané. Rovnaké požiadavky sa vzťahujú aj na všetkých zamestnancov, zúčastňujúcich sa práce s počítačovými systémami. Musia byť definované a opísané úlohy vedenia testovacieho pracoviska, útvaru zabezpečenia kvality, vedúceho štúdie a zamestnancov, ktorí používajú alebo udržiavajú počítačový systém.

17. Pri validácii systému, alebo pri práci s validovaným systémom musí byť podľa možnosti úzka spolupráca medzi príslušnými zamestnancami, akými sú napríklad vedenie testovacieho pracoviska, vedúci štúdie, pracovníci útvaru zabezpečenia kvality, pracovníci IT a pracovníci vykonávajúci validácie. Všetci zamestnanci musia mať primeranú kvalifikáciu a tiež primeranú úroveň prístupu a definované zodpovednosti, potrebné pre vykonávanie im zverených úloh.

18. Zamestnanci, ktorí validujú, prevádzkujú a udržiavajú počítačový systém, sú zodpovední za vykonávanie svojich činností v súlade so zásadami SLP, smernicami správnych praxí a normami. (viď "Referencie" v kapitole 5.5).

19. Úlohy a zodpovedností počas validácie počítačových systémov a vykonávania SLP štúdií, musia byť definované a kontrolované pomocou prístupových práv do systému, školení a všeobecných požiadaviek SLP. Musia byť k dispozícii záznamy o školeniach

a povolenia na prístup do systému pre jednotlivých užívateľov, ktoré musia preukázať, že zamestnanci majú vedomosti a prístupové práva, dostatočné pre plnenie príslušných úloh spôsobom, ktorý je v súlade so zásadami SLP.

20. Príslušné zmluvy alebo dohody o úrovni služieb musia podrobne špecifikovať požiadavky na školenia v oblasti SLP pre globálne alebo korporačné IT tímy, alebo pre externých a interných poskytovateľov IT služieb, ktorí môžu pracovať podľa iných systémov manažérstva kvality ako SLP.

21. Úlohy a zodpovednosti sú opísané v Prílohe 1.

5.1.3.1. Vedenie testovacieho pracoviska

22. Vedenie testovacieho pracoviska nesie celkovú zodpovednosť za to, aby boli k dispozícii také zariadenia, vybavenie, pracovníci a postupy, ktoré zabezpečia, že budú počítačové systémy zvalidované a udržiavané validované.

23. Toto zahŕňa:

a. zodpovednosť za zavedenie postupov, zabezpečujúcich, že počítačové systémy sú vhodné pre zamýšľaný účel a sú prevádzkované a udržiavané v súlade so zásadami SLP;
b. menovanie a efektívne riadenie adekvátneho počtu primerane kvalifikovaných a skúsených zamestnancov; a
c. povinnosť zabezpečiť, aby zariadenia, vybavenie a postupy nakladania s dátami spĺňali adekvátny štandard.

24. Vedenie testovacieho pracoviska musí zabezpečiť, aby postupy požadované na vytvorenie a udržiavanie validovaného stavu počítačových systémov boli pochopené a dodržiavané a zabezpečiť, aby fungoval efektívny monitoring súladu.

25. Vedenie testovacieho pracoviska musí určiť pracovníkov so špecifickou zodpovednosťou za vývoj, validovanie, prevádzkovanie a udržiavanie počítačových systémov. Títo pracovníci musia mať vhodnú kvalifikáciu, dostatočné skúsenosti a primerané školenia, aby plnili svoje povinnosti v súlade so zásadami SLP.

26. Je celkovou zodpovednosťou vedenia testovacieho miesta zabezpečiť, aby počítačové systémy poskytnuté v rámci širšej spoločnosti (testovacieho pracoviska), boli prevádzkované a udržiavané aj na testovacom mieste v súlade so zásadami SLP. Písomné dohody medzi manažmentom miestneho testovacieho pracoviska a materskou organizáciou musia jasne určiť, kto bude zodpovedný za validáciu a udržiavanie validovaného stavu počítačových systémov a ich prevádzku v súlade so zásadami SLP. Vedenie testovacieho pracoviska môže delegovať zodpovednosti, úplne alebo čiastočne, na jednotlivé úrovne systému, alebo kolektívne na primerane zaškolených pracovníkov (napr. celkovú zodpovednosť za súlad počítačových systémov so zásadami SLP na majiteľa systému, alebo za špecifický počítačový systém na vedúceho validácie tohto systému).

27. Vedenie testovacieho pracoviska musí definovať úlohy a zodpovednosti ako za činnosti validácie, tak aj za rutinnú prevádzku každého počítačového systému, bez ohľadu na jeho úroveň komplexnosti. Aby sa predišlo riziku ohrozenia integrity údajov, musia byť prehodnotené potenciálne konflikty záujmov spojené s úlohami a zodpovednosťami

(napr. pracovníci analytického laboratória nesmú mať prístup k nastaveniu audit trail systému, s ktorým pracujú).

5.1.3.2. Vedúci štúdie

28. Vedúci štúdie je zodpovedný za celkové vedenie štúdií a ich súlad so zásadami SLP. Zodpovednosťou vedúceho štúdie je zabezpečiť, aby všetky počítačové systémy používané v štúdiách boli validované a primerane používané. Zodpovednosť vedúceho štúdie za elektronické údaje je taká istá, ako za údaje, zaznamenané v papierovej forme (údaje musia byť vysledovateľné, čitateľné, aktuálne zaznamenávané, pôvodné, presné, kompletné, konzistentné, trvalé a musia byť k dispozícii). Pred začatím štúdie SLP musí vedúci štúdie overiť (verifikovať) stav validácie všetkých počítačových systémov, ktoré budú v štúdii používané.

5.1.3.3. Zabezpečenie kvality

29. Pracovníci útvaru zabezpečenia kvality musia mať prehľad o všetkých, pre SLP relevantných, počítačových systémoch v testovacom pracovisku alebo v testovacom mieste. Vedením testovacieho pracoviska musia byť definované a opísané v písomných postupoch zodpovednosti útvaru zabezpečenia kvality za počítačové systémy. Pracovníci útvaru zabezpečenia kvality musia byť schopní overiť správne použitie validovaných počítačových systémov. Program zabezpečenia kvality musí obsahovať postupy a metódy, ktoré preverujú, či sú, vo všetkých fázach životnosti systému, plnené stanovené požiadavky. Úlohy, súvisiace s preverením požiadaviek pri validácii, prevádzke a udržiavaní počítačových systémov, môžu byť delegované na expertov alebo odborných audítorov (napr. administrátorov systému, majiteľov systému, externých expertov, atď.). Pracovníkom útvaru zabezpečenia kvality musí byť poskytnuté primerané zaškolenie a prístupové práva, ktoré im v prípade potreby umožnia skontrolovať špecifické počítačové procesy (preverenie audit trail, techniky pre analýzy údajov, atď.). Počas inšpekcií štúdií musia mať pracovníci útvaru zabezpečenia kvality priamy prístup „iba na čítanie“ k údajom, pokiaľ sú tieto údaje k dispozícii iba v počítačovom systéme.

30. Vedúci štúdií a pracovníci útvaru zabezpečenia kvality musia mať dostatočné školenie na to, aby rozumeli príslušným postupom, adekvátnym pre počítačové systémy, používané v SLP.

5.1.4 Priestory

31. Primeraná pozornosť musí byť venovaná fyzickému umiestneniu počítačového hardvéru, periférnych komponentov, komunikačného zariadenia a elektronických pamäťových médií. Musí sa predchádzať extrémnym teplotám, vlhkosti, prachu, elektromagnetickým interferenciám a blízkosti vysokonapäťových vedení, pokiaľ zariadenie nie je špeciálne navrhnuté pre prácu v takýchto podmienkach,

32. Taktiež sa musí zvážiť napájanie počítačového zariadenia elektrickou energiou a tam, kde je to vhodné, zabezpečiť zálohovanie alebo neprerušiteľné dodávky energie pre počítačové systémy, výpadok ktorých by mohol ovplyvniť výsledky štúdie. Musia byť zabezpečené primerané priestory pre bezpečné uchovávanie elektronických pamäťových médií.

5.1.5 Inventarizácia

33. Aktuálny zoznam (inventárny súpis) všetkých, pre SLP dôležitých počítačových systémov a ich funkcionalita musí byť udržiavaný. Zoznam musí zahŕňať všetky počítačové systémy, ktoré sú dôležité pre SLP, bez ohľadu na ich komplexnosť. Počítačové systémy používané v SLP musia byť vysledovateľné od plánu štúdie, alebo relevantnej metódy až po inventárny zoznam. Inventárny zoznam musí obsahovať stav validácie, značku, model alebo verziu, podľa toho, čo je vhodné, a majiteľa zariadenia a IT systému. (osoby, ktoré sú priamo zodpovedné za systém).

5.1.6 Dodávateľ

34. Keď sa na zabezpečenie, inštaláciu, konfigurovanie, integrovanie, validovanie, udržiavanie, modifikáciu alebo vyradenie z používania, alebo na služby, akými sú spracovanie údajov, uchovávanie údajov, archivovanie alebo cloud služby, používajú dodávatelia (napr. tretie strany, predávajúci, interné oddelenia IT, poskytovatelia služieb, vrátane poskytovateľov hostingových služieb), potom medzi testovacím pracoviskom a dodávateľom musia existovať písomné dohody (zmluvy). Tieto dohody musia obsahovať jasné informácie, vymedzujúce zodpovednosti dodávateľa, ako aj jasné informácie o vlastníctve údajov.

Pozn. SNAS: Poznámka pod čiarou originálneho dokumentu: „Je na uvážení príslušných orgánov monitorujúcich súlad so zásadami SLP, či zahrnú hostované služby do inšpekčných činností. Orgán monitorujúci súlad môže požiadať poskytovateľa služieb o dokumentáciu alebo vykonať inšpekciu infraštruktúry hostovaných služieb.“

35. Vedenie testovacieho pracoviska musí vyhodnotiť kompetentnosť a spoľahlivosť dodávateľa. Potreba a rozsah zhodnotenia predajcu musia byť založené na hodnotení rizika, berúc do úvahy komplexnosť počítačového systému a kritickosť procesov, podporovaných počítačovým systémom. Potreba auditu sa musí zakladať na zdokumentovanom hodnotení rizika. Je zodpovednosťou vedenia testovacieho pracoviska, aby na základe hodnotenia rizika odôvodnilo požiadavku na audit a jeho typ.

36. Pokiaľ sa rozsah hodnotenia vzťahuje ako na technickú stránku, tak aj na hodnotenie súladu, potom sa musí uvažovať o zaangažovaní odborných technických pracovníkov, ako aj pracovníkov útvaru zabezpečenia kvality. Vedenie testovacieho pracoviska musí vedieť poskytnúť inšpektorom informácie o systéme kvality dodávateľov v závislosti na službách, ktoré títo poskytujú. Dodávatelia nemusia dodržiavať nariadenia pre SLP, ale musia pracovať podľa zdokumentovaného systému kvality, ktorý je vedením testovacieho pracoviska, na základe zhodnotenia útvarom zabezpečenia kvality, potvrdený ako akceptovateľný.

37. V prípade systémov dodávaných predajcom je pravdepodobné, že veľká časť dokumentácie, vytvorenej v priebehu vývoja, bude uchovávaná u predajcu. Pokiaľ je dokumentácia u predajcu, vedenie testovacieho pracoviska sa musí ubezpečiť, že je bezpečne uchovaná. Toto môže vyžadovať formálnu zmluvu medzi predajcom a testovacím pracoviskom. V tomto prípade musí byť v testovacom pracovisku dôkaz o oficiálnom hodnotení a/alebo auditoch predajcu. Vyžaduje sa, aby testovacie pracovisko vykonalo oficiálne akceptačné testovanie systémov dodaných predajcom.

38. Vedenie testovacieho pracoviska musí v písomných dohodách definovať prepojenie medzi svojimi validačnými postupmi a činnosťami, ktoré zabezpečuje dodávateľ. Tieto prepojenia by mali byť aplikovateľné na fázu validácie a fázu prevádzky. Napríklad, akékoľvek testovanie vykonané dodávateľom musí byť zhodnotené vedením testovacieho pracoviska.

39. Hostované služby (napr. platforma, softvér, uchovávanie údajov, archivovanie, zálohovanie alebo procesy vo forme služby) musia byť riešené ako akékoľvek iné, dodávateľom poskytované služby, a vyžadujú si písomné dohody, opisujúce úlohy a zodpovednosti každej strany. Zodpovednosťou vedenia testovacieho pracoviska je vyhodnotiť príslušnú službu a odhadnúť riziká pre integritu a dostupnosť údajov. Vedenie testovacieho pracoviska si musí uvedomovať prípadné riziká, vyplývajúce z nekontrolovaného používania hostovaných služieb.

40. Testovacie pracovisko môže zaradiť IT oddelenie spoločnosti ako súčasť svojho SLP pracoviska. V takýchto prípadoch musia mať prístup na podávanie hlásení vedeniu testovacieho pracoviska.

5.1.7 Komerčné produkty (COTS)

41. Počítačové systémy môžu byť, plne alebo čiastočne, založené na komerčných produktoch - COTS (Commercial Off-The-Shelf). COTS produkty môžu byť používané bez akýchkoľvek modifikácií, s obmedzenou konfiguráciou, s rozsiahlym prispôsobením, alebo dokonca s vlastným programovaním. Tak, ako u ktoréhokoľvek iného typu softvéru, produkty COTS si vyžadujú primeranú validáciu v závislosti od rizika a komplexnosti jednotlivých prispôsobení. Pokiaľ aplikácia (napríklad tabuľka Excel) nie je zložitá, dostatočným je overenie funkcií podľa špecifikácie požiadaviek užívateľa.

42. Špecifikácia požiadaviek užívateľa musí byť v písomnej forme pre všetky aplikácie, ktoré sú založené na produkte COTS. Dokumentácia dodaná s komerčným produktom (COTS) musí byť verifikovaná vedením testovacieho pracoviska, aby bolo isté, že splní špecifikáciu požiadaviek užívateľa.

43. Vzorové tabuľky pre výpočty, využívajúce preddefinované vzorce, vlastnoručne zadané rovnice alebo makrá, sú považované za in-house aplikácie. Požiadavky na ich validáciu sú opísané v časti 2 a 3 a budú závisieť od rizika a komplexnosti. Základné produkty COTS vyžadujú primeranú formu kvalifikácie a jej zdokumentovania. Len kvalifikácia samotná nie je dostačujúca.

5.1.8 Riadenie zmien a konfigurácie

44. Akékoľvek zmeny v počítačovom systéme musia byť robené kontrolovaným spôsobom a v súlade s písomnými postupmi riadenia zmien. Postupy riadenia zmien musia pokrývať fázu validácie, fázu prevádzky (vrátane archivovania) a fázu, v ktorej je systém vyradený z prevádzky. Vedenie testovacieho pracoviska musí zadefinovať úlohy a zodpovednosti pre tých, ktorí sú zaangažovaní na činnostiach riadenia zmien. Rozhodnutie o požiadavkách na riadenie zmien musí byť založené na hodnotení rizika a bude závisieť od zložitosti a kritickosti zmeny pre integritu údajov alebo obchodné

procesy podporované počítačovým systémom. Hodnotenie rizík používané pri riadení zmeny môže využívať kategorizáciu softvéru tak, ako je opísaná v aktuálnej verzii ISPE (International Society for Pharmaceutical Engineering) GAMP (Good Automated Manufacturing Practice) smernice.

45. Kontrola zmien sa musí týkať akýchkoľvek položiek, ktoré prechádzajú revíziou, schválením a testovaním a ktoré sú relevantné pre definovanú konfiguráciu počítačového systému. Konfigurácia systému musí byť vždy presne opísaná a dokumentovaná. Činnosti špecifické pre štúdiu (napr. zhromažďovanie údajov, výpočet údajov, atď.) musia byť vysledovateľné ku konkrétnej konfigurácii počítačových systémov, ak je táto konfigurácia relevantná pre výsledky. Riadenie zmien musí byť prepojené s hodnotením rizík, testovaním, uvoľnením a zodpovedajúcimi postupmi dokumentovania.

Pozn. SNAS:

Traceability (vysledovateľnosť) - znamená, že všetky aktivity súvisiace so štúdiou musia byť spojiteľné s konkrétnou konfiguráciou počítačového systému, najmä ak táto konfigurácia môže ovplyvniť výsledky, napr. verzia OpenLab/Agilent ChemStation pri HPLC alebo verzia Excel tabuľky, ktorou bol robený výpočet.

Change control (riadenie zmien) - zabezpečuje, že každá zmena je dôkladne posúdená a riadne zdokumentovaná, čo minimalizuje riziko ovplyvnenia integrity údajov.

5.1.9 Požiadavky na dokumentáciu

46. Požiadavky na dokumentáciu počítačových systémov musia byť zahrnuté v systéme manažérstva kvality a musia sa vzťahovať na všetky počítačové systémy súvisiace s SLP. Rozsah potrebnej dokumentácie sa bude meniť v závislosti na zložitosti a stratégii validácie počítačového systému. Pre každý počítačový systém musí existovať dokumentácia obvykle zahŕňajúca:

a) názov a verziu softvéru počítačového systému alebo identifikačný kód a podrobný a jasný opis účelu počítačového systému;
b) hardvér, v ktorom je softvér používaný;
c) operačný systém a iný systémový softvér (napr. nástroje), používaný spoločne s počítačovým systémom;
d) programovací jazyk (jazyky) počítačového systému a/alebo používané databázové nástroje (iba tam, kde je to primerané);
e) hlavné funkcie vykonávané počítačovým systémom;
f) prehľad typu a toku údajov, súvisiacich s počítačovým systémom;
g) štruktúry súborov, chybové a výstražné hlásenia súvisiace s používaním počítačového systému;
h) komponenty softvéru počítačového systému s číslami verzií; a
i) konfiguračné a komunikačné linky medzi modulmi počítačového systému a medzi zariadením a inými systémami.

47. Použitie počítačových systémov musí byť primerane dokumentované. Takáto dokumentácia obvykle zahŕňa, ale neobmedzuje sa na:

a) postupy pre prevádzku počítačových systémov (hardvéru a softvéru) a zodpovednosti zapojeného personálu;
b) postupy bezpečnostných opatrení pre odhalenie a prevenciu nepovoleného prístupu alebo zmien v údajoch;
c) postupy riadenia zmien, opisujúce procesy autorizovania, testovania a dokumentovania zmien v zariadení (hardvér and softvér);
d) postupy pre periodické hodnotenie správneho fungovania celého systému alebo jeho komponentov a zaznamenávanie týchto testov;
e) postupy zahŕňajúce rutinnú preventívnu údržbu a opravu chýb (tieto postupy musia jasne a podrobne uvádzať úlohy a zodpovednosti zúčastnených pracovníkov. Pre systémy COTS je akceptovateľné použitie vlastných metód a postupov predajcu pri výkone práce tam, kde je to vhodné. Toto musí byť podrobne opísané v písomnej dohode o úrovni služieb);
f) postupy pre vývoj softvéru, akceptačné testovanie a iné relevantné testovanie a zaznamenávanie všetkých testovaní;
g) postupy zálohovania a postupy na zaistenie kontinuity činnosti;

Pozn. SNAS:
Back-up (zálohovanie) - zahŕňa pravidelné kopírovanie a uchovávanie dôležitých dát a informácií, aby boli chránené v prípade straty, poškodenia, alebo zlyhania primárnych systémov.
Business continuity (kontinuita podnikania) - plánovanie a postupy, ktoré zabezpečujú, že organizácia môže pokračovať v prevádzke aj v prípade vážnych narušení, ako sú napríklad výpadky IT systémov, prírodné katastrofy alebo iné krízové situácie.
Tieto postupy sú kritické pre zabezpečenie toho, že spoločnosť bude schopná rýchlo obnoviť svoju činnosť a minimalizovať škody v prípade nečakaných udalostí.

h) postupy pre archivovanie a „spätné obnovenie“ všetkých elektronických údajov, verzií softvéru a dokumentovanie konfigurácie počítača a dôkazy o všetkých činnostiach;
i) postupy pre monitorovanie a auditovanie počítačových systémov a dôkaz o všetkých činnostiach; a
j) postupy a autorizácie pre vyradenie systému.

48. Pokiaľ je to relevantné, musia byť opísané ďalšie postupy pre riadenie a validáciu a môžu zahŕňať, ale nie sú obmedzené len na: nákup; riadenie rizík; riadenie služieb; plánovanie validácie; špecifikáciu požiadaviek; špecifikáciu dizajnu; inštaláciu; uvoľnenie systému do používania; vysledovateľnosť; riadenie incidentov v IT oblasti; riadenie konfigurácie; riadenie záznamov; zamestnancov; úlohy a zodpovednosti pracovníkov a riadenie dokumentácie.

Pozn. SNAS:

Incident management – riadenie incidentov je proces identifikácie, analýzy a riešenia IT incidentov, ktoré narušujú alebo môžu narušiť bežnú prevádzku organizácie. Cieľom riadenia incidentov je obnoviť normálnu prevádzku čo najrýchlejšie a minimalizovať vplyv na všetky v tom čase vykonané operácie.

49. Musia byť k dispozícii záznamy a postupy ktoré dostatočne podrobne opisujú validáciu a používanie počítačového systému. Tieto záznamy môžu zahŕňať, ale nie sú

obmedzené len na: hodnotenie rizík; hodnotenie dodávateľa; dohody o úrovni služby; špecifikácie požiadaviek užívateľa; testovanie; uvoľňovanie; školenie zamestnancov a používateľov; opis havarijných situácií a zmien; konfiguráciu a prevádzku.

50. Kompletná dokumentácia z validácie a prevádzky počítačového systému musí byť k dispozícii po takú dobu, po akú budú musieť byť v súlade s platnými nariadeniami archivované systémom generované údaje zo štúdie.

5.2 PROJEKTOVÁ FÁZA

5.2.1 Validácia

51. Počítačové systémy musia byť navrhnuté a musí byť preukázané, že vyhovujú pre účely SLP a že boli zavedené vopred naplánovaným spôsobom. Validácia počítačového systému, jej dokumentovanie a správy musia pokrývať jednotlivé kroky životného cyklu, ako je zadefinované vedením testovacieho pracoviska na základe zložitosti a zamýšľaného použitia systému. Úroveň validácie by mala byť odstupňovaná a prispôsobená typu systému a odôvodnená zdokumentovaným hodnotením rizík. Pri odstupňovaní úrovne validácie sa vedenie testovacieho pracoviska môže riadiť metodikami najlepších praktík. Vedenie testovacieho pracoviska musí byť schopné, na základe hodnotenia rizík, zdôvodniť navrhnutý životný cyklus, stratégiu, postupy validácie, protokoly, akceptačné kritériá, postupy, záznamy a zodpovedajúce výstupy. Napríklad výstupy validácie, ktoré poskytuje manažment testovacieho pracoviska, môžu byť obmedzené na špecifikácie požiadaviek používateľa, plán validácie, testovanie používateľskej akceptácie a správu o validácii, ak to môže byť zdôvodnené hodnotením rizík.

52. Musí byť dôkaz o tom, že bola adekvátne otestovaná zhoda systému s kritériami akceptácie, stanovenými vedením testovacieho pracoviska pred uvedením do rutinného používania. Oficiálne akceptačné testovanie vyžaduje, aby boli testy vykonané podľa vopred stanoveného plánu a boli uchované dokumentované dôkazy o všetkých postupoch testovania, údaje z testovania, výsledky testov, oficiálne zhrnutie testovania a záznam o oficiálnej akceptácii.

5.2.2 Kontrolovanie zmien vo fáze validácie

53. Od začiatku procesu validácie musí byť zavedený proces kontrolovania zmien a riadenia odchýlok. Pokiaľ záznamy z kontrolovania zmien a odchýlok nie sú pokladané za relevantné, vedenie testovacieho pracoviska to musí zdôvodniť na základe hodnotenia rizík (napr. zjednodušený prístup k validácii menej komplexného, t. j. jednoduchého, systému).

54. Kontrola zmien počas vývoja a validácie systému musí byť jasne odlíšená od kontroly zmeny počas prevádzky systému. Dokumentácia z validácie musí zahŕňať záznamy z kontroly zmeny (pokiaľ je aplikovateľné) a záznamy o všetkých odchýlkach, zistených v priebehu validačného procesu.

5.2.3 Opis systému

55. K dispozícii musí byť opis systému, s podrobným uvedením fyzického a logického usporiadania, tokov dát a prepojení s inými systémami alebo procesmi, všetkých požiadaviek hardvéru a softvéru, ako aj bezpečnostných opatrení. V priebehu celej životnosti systému musí byť udržiavaný aktualizovaný opis systému tak, ako je opísané v kapitole 5.1.9. Pre jednoduché systémy s nízkou zložitosťou je akceptovateľný aj menej podrobný opis.

5.2.4 Špecifikácia požiadaviek používateľa

56. Špecifikácia požiadaviek používateľa má najvyšší význam pre všetky činnosti súvisiace s validáciou a musí byť vypracovaná pre všetky počítačové systémy súvisiace so SLP, bez ohľadu na zložitosť systému. Špecifikácia požiadaviek používateľa musí opisovať funkcie systému a musí byť založená na dokumentovanom obchodnom procese pre systém a na aplikovateľných regulačných požiadavkách. Úvodné hodnotenie rizika validácie musí byť založené na pochopení obchodných procesov, špecifikácii požiadaviek zo strany používateľa a regulačných požiadaviek.

57. Špecifikácia požiadaviek zo strany používateľa musí zahŕňať všetky, pre SLP relevantné, funkcie systému a musí byť použitá pri hodnotení rizika, aby sa identifikovali rozhodujúce funkcie a vhodné testovacie činnosti. V závislosti na zložitosti systému musia byť špecifikácie požiadaviek používateľa nadväzujúce na všetky ďalšie dokumenty špecifikácie (ak je to potrebné) a dokumentáciu z testovania, vytvorenú počas celej životnosti počítačového systému.

58. Pokiaľ poskytnutý systém (zakúpený, alebo hostovaný dodávateľom) obsahuje viac funkcií než je potrebné, testované musia byť iba funkcie, relevantné pre SLP. Validácia musí tiež zahŕňať funkcie, ktoré môžu byť používané pri nie-SLP štúdiách a ktoré by mohli zasahovať do použitia počítačového systému pri štúdiách SLP. Ostatné funkcie a/alebo funkcionality, ktoré sú mimo rozsahu (t.j. nie sú plánované na použitie) musia byť identifikované, avšak ich testovanie sa nevyžaduje.

5.2.5 Systém manažérstva kvality a podporné postupy

59. Vývoj počítačového systému, ako aj proces validácie, musí byť riadený systémom manažérstva kvality. K dispozícii musí byť adekvátna dokumentácia dosvedčujúca, že systém bol vyvinutý kontrolovaným spôsobom a pokiaľ možno, v súlade s uznávanými normami kvality a technickými normami (napr. ISO 9001). Pokiaľ je systém vyvíjaný predajcom, je zodpovednosťou vedenia testovacieho pracoviska, aby vyhodnotilo predajcov systém manažérstva kvality pre systém vývoja. Testovacie pracovisko sa pri definovaní stratégie vyhodnocovania musí opierať o hodnotenie rizika.

5.2.6 Špeciálne vyvinuté systémy

60. Špeciálne vyvinuté systémy sú vyvinuté pre špecifické využitie v konkrétnom testovacom pracovisku (napr. systémy na zhromažďovanie špecifických údajov v rámci štúdie SLP, šablóny tabuľkových procesorov so vzorcami alebo makrami, otázky, štatistické aplikácie alebo systémy na vyhodnocovanie údajov, atď.). Takéto počítačové systémy musia tiež byť konfigurované alebo kódované špecificky pre jednu alebo viac SLP štúdií. Keďže nie sú k dispozícii žiadne skúsenosti z predchádzajúcich alebo paralelných použití, špeciálne vyvinuté systémy prinášajú najväčšie skutočné riziko. Musí byť zavedený proces pre validáciu špeciálnych počítačových systémov, zabezpečujúci formálne hodnotenie a nahlasovanie opatrení pre kvalitu a výkonnosť počas všetkých štádií životnosti systému.

Pozn. SNAS: V poznámke pod čiarou je uvedené: „V niektorých členských krajinách OECD by mal byť zdrojový kód prispôsobených systémov (alebo všetkého softvéru počítačového systému) dostupný pre manažment testovacieho pracoviska, aby mohol poskytnúť prístup monitorovaciemu orgánu k softvérovému kódu. To možno dosiahnuť archiváciou digitálnej kópie zdrojového kódu, dohodou o úschove (escrow arrangements) alebo písomnými dohodami.“, tento prístup nie je právnymi predpismi SR zatiaľ požadovaný.

61. Potrebná je písomná dohoda medzi dodávateľom špeciálneho vyvinutého systému a vedením testovacieho pracoviska, opisujúca relevantné úlohy a zodpovednosti pri validácii takéhoto systému. Pri validácii musí vedenie testovacieho pracoviska vziať do úvahy všetky s kvalitou súvisiace činnosti dodávateľa, vykonané aj v mieste dodávateľa. Súčasťou životného cyklu počítačového systému majú byť aj všetky outsorcované činnosti alebo interné aktivity dodávateľa.

62. Pokiaľ je aplikácia na hostiteľskom systéme aplikáciou s vlastným kódovaním alebo je konfigurovaná, systém je treba posudzovať aj ako špeciálny, ale aj ako predávajúcim dodaný systém.

5.2.7 Testovanie

63. Testovanie (napr. testovanie pri inštalácii, akceptačné testovanie klientom) musí byť uskutočnené tak, aby sa zabezpečilo, že systém bude spĺňať vopred definované požiadavky. Je zodpovednosťou vedenia testovacieho pracoviska porozumieť potrebe testovania a zabezpečiť kompletnosť testov a dokumentácie z testovania. Testovanie musí byť založené na znalosti obchodného procesu a zamýšľaného spôsobu použitia systému. Postupy musia opisovať, ako sa vykonajú testy a jasne definovať úlohy a zodpovednosti, ako aj požiadavky na dokumentáciu. Testovacie pracovisko je zodpovedné za prijatie rozhodnutia o hĺbke a rozsahu testovania, ktoré sa bude riadiť hodnotením rizika. Vedenie testovacieho pracoviska musí zabezpečiť, že všetky systémy, vrátane systémov COTS sú testované a vyhodnotené. Pri validovaní môžu vedeniu testovacieho pracoviska pomôcť vykonané testy a dokumentácia dodávateľa a môžu doplniť alebo nahradiť testovanie v testovacom pracovisku. Vedenie testovacieho pracoviska musí mať dôkazy z testovania bez ohľadu na to, či bolo testovanie vykonávané testovacím pracoviskom alebo dodávateľ preukáže, ktoré relevantné metódy testovania

a scenáre testovania boli použité. Obzvlášť je potrebné zohľadniť limity parametrov systému (procesu), limity údajov a spracovanie chýb.

64. Vedenie testovacieho pracoviska musí zvážiť spôsob špecifického akceptačného testovania používateľom, aby sa preukázalo, že systém je vhodný na vykonávanie špecifickej štúdie SLP (napr. overiť vhodnosť systému, vykonávajúceho typické analytické stanovenie vrátane kalibrácie, meraní, výpočtov a prenosu údajov do LIMS).

65. Musia existovať postupy pre kontroly zmien. Pokiaľ testovanie vedie k systémovým zmenám, tieto musia byť riadené prostredníctvom kontroly zmien. Dôkaz o adekvátnosti testovania môže byť zabezpečený prostredníctvom udržiavania záznamov o výsledkoch interného testovania alebo záznamov z auditu dodávateľa.

5.2.8 Prenos údajov

66. K prenosu/migrácii údajov môže dôjsť v priebehu štúdie SLP, alebo po jej ukončení. Prenos údajov musí byť súčasťou rozsahu validácie stanoveného vedením testovacieho pracoviska, pokiaľ sa táto migrácia dotýka údajov relevantných pre SLP, a to bez ohľadu na stav ktoréhokoľvek projektu štúdie SLP. Pokiaľ sú záznamy zo štúdie archivované v elektronickom systéme, prenos údajov sa môže stať relevantným.

67. Tam, kde sa elektronické údaje prenášajú z jedného systému do druhého, proces musí byť dokumentovaný. Vedenie testovacieho pracoviska zodpovedá za zabezpečenie a preukázanie toho, že údaje počas prenosu nebudú zmenené. Konvertovanie údajov do iného formátu sa tiež považuje za prenos údajov (napr. z formátu vlastníckych údajov do PDF). Tam, kde sa údaje prenášajú na iné médium, musí byť pred akýmkoľvek zničením originálnych údajov overené, že sú tieto údaje presnou kópiou pôvodných údajov.

68. Náročnosť prenosu údajov sa môže značne líšiť v jeho zložitosti a rizikách. Príklady zahŕňajú:

a) upgrade verzie;
b) konverzie údajov (z jednej databázy do druhej; do iného formátu dát; zmena formátu súvisiaca s aktualizáciou softvéru);
c) prenos v rámci toho istého systému (prenos aplikácie; údaje z jedného servera do druhého); a
d) prenos zo zdrojového do cieľového systému.

69. Prenesené údaje musia zostať použiteľné a musia si uchovať svoj obsah a význam. Hodnota a/alebo význam a prepojenia medzi audit trail systému a elektronickými podpismi musia byť v rámci migračného procesu zabezpečené. Zodpovednosťou vedenia testovacieho pracoviska je udržať prepojenie medzi čitateľným audit trail alebo elektronickými podpismi a auditovanými údajmi.

5.2.9 Výmena údajov

70. Komunikácie súvisiace s počítačovými systémami vo všeobecnosti spadajú do dvoch kategórií: komunikácia medzi počítačmi alebo medzi počítačmi a periférnymi komponentmi. Údaje relevantné pre SLP môžu byť prenášané automaticky, jednosmerne

alebo dvojsmerne, z jedného systému do druhého systému (napr. z vzdialeného systému na zber údajov do centrálnej databázy, z tabuľkového kalkulátora do LIMS, zo systému riadenia chromatografických údajov do LIMS, alebo z tabuľkového kalkulátora do štatistickej softvérovej aplikácie). Všetky komunikačné spojenia sú potenciálnym zdrojom chyby a môžu mať za následok stratu alebo poškodenie údajov. Pre bezpečnosť a integritu systému je v priebehu vývoja, validácie, prevádzky a údržby potrebné primerane vyriešiť aj vhodné kontroly prepojení. Výmena elektronických údajov medzi systémami musí zahŕňať vhodné zabudované kontroly pre správnosť a bezpečnosť vstupov a spracovanie dát. Infraštruktúra siete musí byť kvalifikovaná. Účelom tejto požiadavky však nie je vyžadovať validáciu štandardnej komunikačnej infraštruktúry a jej postupov (napr. základný komunikačný jazyk internetu TCP/IP [Transmission Control Protocol / Internet Protocol]).

5.3 FÁZA PREVÁDZKY

71. Všetky počítačové systémy musia byť prevádzkované a udržiavané spôsobom, zabezpečujúcim kontinuitu ich validovaného stavu.

5.3.1 Kontrola správnosti

72. Vedenie testovacieho pracoviska musí vedieť o všetkých, pre SLP relevantných údajoch, zadávaných manuálne do počítačového systému. Zodpovednosťou vedenia testovacieho pracoviska je primerane kontrolovať každý systém elektronického zadávania údajov, bez ohľadu na jeho zložitosť. Pre identifikovanie potenciálnej možnosti zadania nesprávnych údajov a vyhodnotenie kritickosti a dôsledkov chybne alebo nesprávne zadaných údajov, musí byť použité hodnotenie rizík. Musia byť opísané a implementované stratégie na zníženie rizika. Toto môže mať za následok potrebu dodatočných ručných a/alebo elektronických kontrol správnosti zadaných údajov druhým operátorom alebo elektronickým systémom. Keď sa používajú, musia byť automatizované kontroly pri zadávaní údajov zahrnuté do validácie počítačových systémov, (napr. automaticky aplikované validačné skripty počas manuálneho zadávania údajov), pričom rozsah validácie by mal byť odstupňovaný na základe posúdenia rizika. Použitie nevalidovaných systémov zadávania údajov musí byť vylúčené (napr. nekontrolované používanie tabuľkových kalkulátorov). Pokiaľ sa na manuálne zadávanie údajov používajú manuálne kontrolné postupy, potom takýto postup má byť zabezpečený adekvátnou dokumentáciou, čo uľahčí rekonštrukciu činností.

5.3.2 Údaje a uchovávanie údajov

73. Pokiaľ sú údaje (primárne údaje, odvodené údaje alebo metadáta) uchovávané elektronicky, musia byť definované požiadavky na ich zálohovanie a archivovanie. Aby bola možná obnova údajov po zlyhaní, ktoré ohrozuje integritu systému, musí byť vykonávané zálohovanie všetkých relevantných údajov.

74. Uchované údaje musia byť pred stratou, poškodením a/alebo zmenou zabezpečené ako fyzickými, tak aj elektronickými prostriedkami. Musí byť preverená obnoviteľnosť, dostupnosť, čitateľnosť a správnosť uložených údajov. Postupy verifikácie uchovávaných údajov musia byť založené na hodnotení rizika. Počas celej doby uchovávania musí byť zabezpečený prístup k uchovaným údajom.

75. Zmeny v systéme hardvéru a softvéru musia umožňovať nepretržitý prístup k údajom a ich udržiavanie bez akéhokoľvek rizika pre integritu údajov. Po aktualizovaní systému alebo softvéru musí byť možné čítať údaje uložené predchádzajúcou verziou, alebo musia byť k dispozícii iné metódy na prečítanie starých údajov. Podporné informácie (napr. záznamy o údržbe, záznamy o kalibrácii, konfigurácia, atď.), ktoré sú potrebné pre overenie platnosti primárnych údajov alebo rekonštrukciu celej štúdie alebo jej časti, musia byť zálohované a udržiavané v archíve. Pokiaľ je potrebné prečítať, alebo zrekonštruovať údaje, v archíve musí byť udržiavaný príslušný softvér.

76. Pokiaľ ide o elektronické záznamy, vedenie testovacieho pracoviska musí:

a) identifikovať všetky elektronické záznamy súvisiace so štúdiou (napr. primárne údaje, odvodené údaje). Je potrebné, aby boli primárne údaje identifikované pre každý počítačový systém bez ohľadu na to, ako s ním primárne údaje súvisia (napr. uchovaním na elektronickom pamäťovom médiu, výtlačmi z počítačov alebo prístrojov, atď.);
b) zhodnotiť kritickosť elektronických záznamov pre kvalitu výsledkov štúdie;
c) zhodnotiť potenciálne riziká pre elektronické záznamy;
d) určiť postupy na znížene rizika; a
e) monitorovať efektívnosť zníženia rizika v priebehu životnosti.

77. Pokiaľ ide o postupy, vedenie testovacieho pracoviska musí opísať, ako sú uchovávané elektronické záznamy, ako je chránená integrita údajov a ako sa udržiava čitateľnosť údajov. Pre každé, pre SLP relevantné časové obdobie, toto zahŕňa, ale nie je obmedzené na:

a) Kontrolu fyzického prístupu k elektronickým pamäťovým médiám (napr. opatrenia pre kontrolu a monitorovanie prístupu osôb do serverovní, atď.);
b) Kontrolu logického (elektronického) prístupu k uchovaným záznamom (napr. koncepcia pridelenia užívateľských práv pre počítačové systémy ako súčasť validácie počítačového systému, ktorá definuje úlohy a prístupové práva v ktoromkoľvek, pre SLP relevantnom počítačovom systéme);
c) Fyzickú ochranu úložných médií pred stratou alebo zničením (napr. požiar, vlhkosť, deštruktívne elektrické poruchy alebo anomálie, krádež, atď.);
d) Ochranu uchovaných elektronických záznamov pred stratou a zmenami (napr. validácia postupov zálohovania, vrátane verifikácie zálohovaných údajov a správneho uchovávania zálohovaných údajov; aplikácia audit trail systémov); a
e) Zabezpečenie dostupnosti a čitateľnosti elektronických záznamov pomocou adekvátneho fyzického, ako aj softvérového prostredia.

78. O uchovávaní údajov sa musí uvažovať pri každom počítačovom systéme, používanom na vykonávanie SLP štúdií a počas obdobia archivácie. Do dokumentácie štúdie nie je potrebné vkladať takéto hodnotenie. Vedenie testovacieho pracoviska však

musí mať politiku na vysvetlenie toho, ako sa uchovávajú údaje a ako sú plnené požiadavky na uchovávanie. Táto informácia musí byť súčasťou dokumentácie o validácii systému. Pokiaľ testovacie pracovisko odovzdáva elektronické údaje zo štúdie objednávateľovi štúdie, zodpovednosť za údaje prechádza naňho.

5.3.3 Tlačené výstupy z počítača

79. Pokiaľ sú údaje vytlačené tak, aby zastupovali primárne údaje, potom musia byť vytlačené všetky elektronické údaje, vrátane odvodených údajov, ako aj metadát (informácií o zmene údajov, pokiaľ sú takéto zmeny potrebné pre udržanie správneho obsahu a významu údajov). Alternatívne musia byť všetky elektronické záznamy aj overiteľné na obrazovke vo formáte, čitateľnom pre ľudí a udržiavané. Toto zahŕňa všetky informácie o zmenách, vykonaných v záznamoch, pokiaľ sú tieto zmeny relevantné pre správny obsah a význam.

5.3.4 Revízne záznamy (Audit trails)

80. Audit trail zabezpečuje dokumentovaný dôkaz o činnostiach, ktoré ovplyvnili obsah alebo význam záznamu v konkrétnom časovom bode. Tieto záznamy musia byť k dispozícii a musia byť skonvertovateľné do formátu čitateľného pre človeka. V závislosti na systéme, môžu pre splnenie tejto požiadavky byť brané do úvahy aj súbory denníka (log files), (alebo môžu byť brané do úvahy ako doplnok k audit trail systému). Žiadna zmena v elektronických záznamoch nesmie prekryť originálny vstup a musia byť označením časom a dátumom vysledovateľné až k osobe, ktorá urobila zmenu.

81. Audit trail pre počítačový systém musí byť aktivovaný (povolený), primerane konfigurovaný a musí odrážať úlohy a zodpovednosti personálu štúdie. Možnosť robiť modifikácie v nastaveniach revíznych záznamov musí byť limitovaná na oprávnených pracovníkov. Žiadny pracovník zaangažovaný v štúdii (napr. vedúci štúdie, vedúci analytického oddelenia, analytici, atď.) nesmie mať povolenie na robenie zmien v ich nastaveniach.

82. Musí byť zavedený systém, ktorý môže, na základe hodnotenia rizika, zabezpečiť preskúmanie funkcií audit trailu, jeho nastavení a zaznamenaných informácií. Pri preskúmaní záznamov audit trailu vedenie testovacieho pracoviska môže zobrať do úvahy, ale neobmedziť sa iba na jednotlivé udalosti (napr. správanie užívateľa, otázky integrity podozrivých údajov). Zvážená musí byť úplnosť a vhodnosť funkcií a nastavení audit trailu. Zaangažovaní musia byť pracovníci zabezpečenia kvality SLP. Preskúmanie funkcií audit trialu musí byť založené na chápaní použitia systému, možnosti modifikovať záznamy a kontrolách zabraňujúcich svojvoľné zmeny záznamov.

83. Systém musí byť schopný upozorniť na zmeny, urobené v skôr zadaných údajoch na obrazovke a vo všetkých tlačených kópiách. Originálny vstup a modifikované vstupy musia byť systémom udržiavané. V niektorých systémoch môžu audit trails existovať ako záznamy zmien, doplňujúce zobrazované údaje (na obrazovke alebo vytlačené). Originálne údaje musia byť uchovávané spolu s modifikovanými údajmi. Napríklad, každý

reintegrovaný chromatogram, zmenený pre účely prepočítania, musí byť nezmeniteľne označený.

5.3.5 Riadenie zmien a riadenie konfigurácie

84. Vedenie testovacieho pracoviska musí mať vhodné postupy pre riadenie konfigurácie a riadenie zmeny vo fáze prevádzky počítačového systému. Riadenie zmeny aj konfigurácie musí byť aplikované na hardvér aj na softvér. Opatrenia na kontrolu zmeny musia zabezpečiť, že zmeny v konfigurácii počítačového systému, ktoré by mohli ovplyvniť jeho validačný stav, budú zavedené kontrolovaným spôsobom. Zmena musí byť vysledovateľná z relevantných záznamov o kontrole zmeny a konfigurácie. Postupy musia opisovať metódu hodnotenia, používanú na určenie rozsahu opätovného testovania, potrebného na udržanie systému vo validovanom stave.

85. Postupy kontroly zmeny musia jasne definovať úlohy a zodpovednosti pre zhodnotenie a schvaľovanie zmien a podrobné postupy pre hodnotenie zmeny. Nezávisle od pôvodu zmeny (systém od dodávateľa alebo vyvinutý in-home), ako súčasť procesu kontroly zmeny musia byť zabezpečené príslušné informácie. Postupy kontroly zmeny musia zabezpečiť integritu údajov.

86. Konfigurácia počítačového systému musí byť známa kedykoľvek v priebehu jeho životného cyklu, od prvého kroku vývoja až po jeho vyradenie. Na preukázanie adekvátneho použitia počítačového systému – bez ohľadu na jeho zložitosť - v štúdii SLP, sa požaduje dokumentovaná zhoda konfigurácie analytického nástroja s ustanoveniami uvedenými vo validácii metódy. Výsledok každej štúdie SLP musí byť vysledovateľný podľa relevantnej a validovanej konfigurácie systému, aby sa umožnilo overenie nastavení, ako sú uvedené v pláne štúdie alebo v relevantnej metóde.

87. Ako reakcia na nehody (udalosti), alebo na špecifické účely zariadenia/štúdie môžu byť potrebné zmeny. Po modifikácii alebo oprave musí byť preverený a zdokumentovaný stav validácie systému.

88. Modifikácie implementované rutinnou automatizáciou (napr antivírusová ochrana alebo záplaty operačného systému) musia byť súčasťou formálnej kontroly zmeny alebo riadenia konfigurácie. Absencia riadenia zmeny v počítačovom systéme musí byť odôvodnená a založená na hodnotení rizík.

5.3.6 Pravidelné preskúmanie

89. Počítačové systémy musia byť pravidelne preskúmavané, aby sa potvrdilo, že sú stále vo validovanom stave, sú v súlade s SLP a naďalej plnia určené kritériá výkonnosti (napríklad spoľahlivosť, citlivosť, kapacita, atď.). Tam, kde je to vhodné, preskúmanie musí zahŕňať aktuálny rozsah funkcií, záznamy o odchýlkach, nehody, históriu aktualizácií (upgradov), výkonnosť, spoľahlivosť a bezpečnosť, ktoré by boli mohli ovplyvniť stav validácie systému. Frekvencia a hĺbka, do ktorej ide pravidelné preskúmanie musia byť určené na základe hodnotenia rizika, s ohľadom na zložitosť a kritickosť pre SLP. Pravidelné preskúmanie musí brať do úvahy každú nahlásenú neočakávanú udalosť, ktorá mohla ovplyvniť stav validácie systému. Vhodnosť činností

súvisiacich s preskúmaním a zaangažovanie odborných špecialistov, ako aj pracovníkov, ktorých sa týka SLP (napr. vedenie testovacieho pracoviska, útvar, zabezpečenie kvality, podporný personál IT, dodávateľ, atď.) musí byť zdôvodnená. Musia byť definované zodpovednosti pracovníkov, zapojených do pravidelného preskúmania stavu validácie počítačového systému. Potreba interakcie medzi činnosťami pravidelného preskúmania a systémom hlásenia nehôd musí byť zvážená v závislosti na hodnotení rizika. Výsledky činností pravidelného preskúmania a tam, kde je to aplikovateľné, činnosti zjednávajúce nápravu, musia byť zdokumentované.

90. Menej kritické a menej zložité počítačové systémy môžu byť vylúčené z preskúmania za predpokladu, že je toto vylúčenie založené na hodnotení rizika. Pravidelné preskúmanie nemusí byť potrebné, pokiaľ bola nedávno vykonaná (re-) validácia a teda je možné preskúmanie odložiť na neskôr. Pokiaľ neboli hlásené žiadne neočakávané udalosti, ktoré by mohli ovplyvniť stav validácie, môžu byť z preskúmania vyradené automatizované systémy COTS. Pravidelné preskúmanie musí byť vykonané vtedy, keď je to požadované (napr. v prípade organizačných zmien), alebo minimálne raz ročne, nakoľko sa osoby a úlohy môžu zmeniť. Pre COTS musí byť tiež vykonaná užívateľská kontrola.

5.3.7 Fyzická, logická bezpečnosť a integrita údajov

91. Pre ochranu hardvéru, softvéru a údajov pred zničením alebo nepovolenou modifikáciou, alebo stratou, musia byť zavedené dokumentované bezpečnostné postupy, schválené testovacím pracoviskom. V závislosti na zložitosti a kritickosti systému a požiadavkách organizácie, v ktorej je systém prevádzkovaný, musia byť zavedené vhodné fyzické a/alebo logické kontroly.

92. Za účelom predchádzania nepovolenému fyzickému vstupu do systému (napr. počítačový hardvér, komunikačné zariadenie, periférne prvky a elektronické pamäťové médiá) musia byť zavedené vhodné metódy kontroly, ktoré môžu zahŕňať používanie kľúčov, prístupových kariet, osobných kódov s heslami, biometrických údajov, alebo obmedzený prístup ku konkrétnemu počítačovému zariadeniu (napr. priestory na uchovávanie údajov, rozhrania, počítače, serverové miestnosti, atď..). Vytvorenie, zmena a zrušenie povolenia na prístup musia byť zaznamenávané. Záznamy o povoleniach musia byť pravidelne preskúmavané na základe kritickosti procesu, podporovaného počítačovým systémom a v prípade relevantných organizačných zmien v testovacom pracovisku.

93. Nakoľko udržiavanie integrity údajov je primárnym cieľom zásad SLP, vedenie testovacieho pracoviska musí zabezpečiť, aby si pracovníci uvedomovali dôležitosť bezpečnosti údajov, funkcie postupov a systému, ktoré sú k dispozícii pre zabezpečenie primeranej bezpečnosti a dôsledky narušenia bezpečnosti. Tieto funkcie systému musia zahŕňať rutinný dohľad nad prístupom do systému, implementáciu rutiny do preverovania súborov a hlásenie výnimiek a/alebo trendov.

94. Pre zariadenia, ktoré nie sú umiestnené v špecifických „počítačových miestnostiach“ (napr. osobné počítače a terminály) musí byť kontrola prístupu do priestorov, kde je umiestnený hardvér (napr. kontrola prístupu do budovy, priestoru laboratória, alebo konkrétnej miestnosti). Tam, kde je takéto zariadenie umiestnené na diaľku (napr.

prenosné komponenty a modemové prepojenia), môžu byť prijaté doplňujúce opatrenia, ktoré musia byť zdôvodnené a musia sa zakladať na hodnotení rizika (napr. kryptografická kontrola).

95. Základom je, aby sa používali iba kvalifikované a schválené verzie softvéru. Každé zavedenie údajov alebo softvéru z externých zdrojov musí byť kontrolované. Tieto kontroly musia byť zabezpečené operačným systémom počítača, osobitnými bezpečnostnými postupmi, rutinnými postupmi, zakomponovanými do aplikácie, alebo ich kombináciou. Systémy pre uchovávanie údajov a dokumentov musia byť navrhnuté tak, aby zaznamenávali dátum, čas a identitu operátora, ktorý zadáva, mení, potvrdzuje alebo vymazáva údaje.

96. Potenciálna možnosť zničenia údajov škodlivým kódom alebo inými prostriedkami musí byť riešená, pokiaľ je to považované za potrebné. Musia byť prijaté bezpečnostné opatrenia na zabezpečenie integrity údajov v prípade krátkodobého aj dlhodobého zlyhania systému.

97. Primeraná a dobre udržiavaná politika udeľovania povolení musí špecifikovať logické prístupové práva do domén, počítačov, aplikácií a k údajom. Pre operačné systémy a aplikácie musia byť definované užívateľské oprávnenia a musia byť prispôsobené požiadavkám, ktoré požaduje organizácia testovacieho pracoviska a konkrétna SLP štúdia. Musia byť definované úlohy a zodpovednosti pracovníkov prideľujúcich užívateľské oprávnenia.

98. Užívateľské oprávnenia v rámci počítačového systému nesmú zasahovať do požiadaviek na integritu údajov. Činnosti všetkých pracovníkov štúdie SLP musia byť vysledovateľné podľa užívateľských oprávnení a činností v rámci všetkých relevantných počítačových systémov a musia byť opísané v dokumentoch užívateľských privilégií. Práva administrátora nesmú byť pridelené osobám, ktoré potenciálne môžu mať záujem o údaje (napr. pozícia „analytik“ v rámci laboratória nie je kompatibilná so systémovou pozíciou „administrátor“ v systéme správy údajov chromatografie). Používateľ by v konkrétnom systéme nemal mať druhú úlohu, ktorá by mohla zasahovať do požiadaviek na integritu údajov.

5.3.8 Riadenie náhodných situácií

99. Pri dennom prevádzkovaní systému musia byť udržiavané záznamy o všetkých zistených problémoch alebo rozporoch a všetkých opatreniach na ich odstránenie. Vedúci štúdie, vedenie testovacieho pracoviska, útvar zabezpečenia kvality a pokiaľ je to vhodné, aj objednávateľ, musia byť informovaní o náhodných situáciách, vyžadujúcich si nápravné činnosti. Vedúci štúdie je zodpovedný za zadefinovanie kritickosti náhodných situácií a za zhodnotenie dopadu na štúdiu. Musí byť identifikovaná kľúčová príčina náhodnej situácie, vyžadujúca nápravnú činnosť a táto vytvorí základ pre nápravné a preventívne opatrenia. Musí byť určená priorita pre nápravné a preventívne opatrenia. Musí byť možné vysledovať všetky náhodné situácie, vyžadujúce nápravné opatrenie nahlásené pre počítačový systém v rámci dotknutej štúdie SLP a naopak.

100. V systémovej dokumentácii musia byť udržiavané a pravidelne archivované záznamy o náhodných situáciách. Záznamy o náhodných situáciách musia byť

uchovávané a skladované spolu s relevantnou (validačnou) dokumentáciou, pretože správy o náhodných situáciách sú potrebné pre monitorovanie a pravidelné preskúmanie. Testovacie pracovisko musí mať riadenie náhodných situácií prepojené, alebo integrované s riadením zmeny, riadením konfigurácie, pravidelným preskúmaním a školením. Preskúmanie vzniknutých náhodných situácií musí byť súčasťou pravidelného hodnotenia systému.

5.3.9 Elektronický podpis

101. Elektronické záznamy môžu byť podpísané elektronicky, pripojením elektronického podpisu.

102. Očakáva sa, že elektronické podpisy:

a. majú také isté právne následky ako ručné podpisy, prinajmenšom v rámci hraníc testovacieho pracoviska;
b. sú trvalo spojené s ich príslušnými záznamami;
c. zahŕňajú čas a dátum, kedy boli použité; a
d. umožnia identifikáciu podpisujúceho a význam podpisu.

103. Funkcia elektronického podpisu počítačového systému musí byť riešená v rámci požiadaviek na systém a validovaná a opísaná v postupoch systému. Vedenie testovacieho pracoviska musí mať identifikované tie záznamy, ktoré si vyžadujú ručný, alebo elektronický podpis. Od rozhodnutia vedenia testovacieho pracoviska závisí, či sa spoľahne na funkciu elektronického podpisu, pokiaľ sú k dispozícii aj iné prostriedky (napr. vytlačenie a podpísanie rukou). Aplikované postupy musia byť adekvátne opísané.

104. Vedenie testovacieho pracoviska musí zabezpečiť zavedenie politiky elektronického podpisu za účelom zabezpečenia adekvátneho použitia a udržiavania funkcií elektronického podpisu počítačového systému. Pracovníci, majúci právo podpisovať elektronicky, musia byť jasne identifikovaní na základe mena a prepojení menom s politikou elektronického podpisu. Úloha osoby v štúdii SLP musí premietnutá do významu príslušného elektronického podpisu, ktorý je aplikovaný počítačovým systémom použitom v štúdii a musí byť vysledovateľná k autorizačnej politike systému. Môže sa stať, že bude potrebné prispôsobiť koncepciu udeľovania povolení počítačového systému požiadavkám konkrétnej štúdie.

105. Vedenie testovacieho pracoviska musí zabezpečiť, že elektronický podpis je ekvivalentom ručného podpisu a jeho pravosť je neodškriepiteľná prinajmenšom v rámci hraníc testovacieho pracoviska alebo testovacieho miesta. Za minimálnu požiadavku pre elektronický podpis musí byť považované opätovné zadanie hesla. Aktivovanie funkčnej klávesy osobou, prihlásenou do systému nemôže byť považované za elektronický podpis.

106. Metadáta, ktoré sú spojené s elektronicky podpísaným záznamom, musia byť jasne identifikované (napr. nastavenia metódy a konfigurácia systému, pokiaľ je toto relevantné pre elektronicky podpísané analytické výsledky, atď.). Funkcia podpisovania v rámci počítačového systému musí zabezpečiť časový prehľad prepojení medzi elektronicky podpísaným záznamom a podpornými metadátami. Užívateľ nesmie mať možnosť zmeniť aplikovaný elektronický podpis, ani prepojenie na súvisiace metadáta. Pokiaľ dôjde k zmene elektronicky podpísaného záznamu alebo podporných metadát,

musí to byť vysvetlené, (elektronicky) podpísané a datované osobou, zodpovednou za zmenu. Vplyv zmeny elektronicky podpísaného záznamu alebo podporujúcich metadát na elektronický podpis musí byť zhodnotený, nakoľko zmena spôsobí neplatnosť pôvodného elektronického podpisu.

107. Vedenie testovacieho pracoviska môže uplatniť „na papieri založený“ postup pre podpisovanie záznamov, ktoré sú vytlačené z elektronického systému. Musí byť uvedené, že papierové výtlačky elektronických záznamov nemusia obsahovať všetky informácie, ktoré sú potrebné pre úplné zrekonštruovanie činností, alebo poskytnutie úplného významu údajov. Určité podporné metadáta, relevantné pre vytlačené/podpísané záznamy môžu byť udržiavané elektronicky (hybridné riešenie). Použitie takéhoto hybridného systému musí byť v plnom rozsahu vysvetlené v postupoch testovacieho pracoviska a odôvodnené prostredníctvom hodnotenia rizík. Na základe hodnotenia rizík musí byť tlač urobená až po jasnom pochopení procesu a informácií, ktoré nebudú vo výtlačku zobrazené. Hybridné riešenie musí byť jasne opísané, aby sa identifikovali všetky dodatočné elektronické záznamy alebo podporné metadáta, ktoré sú reprezentované vytlačenou a podpísanou verziou záznamu. Vhodný systém kontroly verzií musí zabezpečiť aktuálnosť prepojenia medzi vytlačeným/podpísaným záznamom a elektronicky udržiavanými záznamami. Musí byť umožnený prístup k zmeneným, alebo nahradeným (vyradeným) záznamom za účelom vysledovateľnosti zmien a dokumentovanie neplatných výsledkov. Tieto záznamy však musia byť vylúčené z rutinného použitia. Pokiaľ sa paralelne udržiava kompletný súbor elektronických záznamov a ich vytlačená verzia, vedenie testovacieho pracoviska musí špecifikovať, ktorý typ záznamov je riadený, aby sa mohol uplatniť vhodný postup kontroly (napr. pokiaľ je celý súbor informácií z analytického systému vytlačený a zároveň udržiavaný elektronicky, musí byť definované, ktorý súbor informácií je regulovaný).

5.3.10 Schvaľovanie údajov

108. Pokiaľ postup zahŕňa proces elektronického schvaľovania údajov, funkcia schvaľovania údajov musí byť súčasťou validácie systému. Schvaľovací proces musí byť opísaný v postupoch testovacieho pracoviska a musí sa vykonávať elektronicky v rámci systému.

5.3.11 Archivovanie

109. Pokiaľ ide o archivovanie, táto smernica dopĺňa OECD GLP Advisory Document No.15 “Zriadenie a kontrola archívu, ktorý funguje v súlade so zásadami SLP”.

110. Akékoľvek údaje, súvisiace so SLP, môžu byť archivované v elektronickej forme. Zásady SLP pre archivovanie musia byť dôsledne aplikované rovnako na elektronické, ako aj na neelektronické údaje. Preto je dôležité, aby boli elektronické údaje uchovávané na rovnakej úrovni kontroly prístupu, indexovania a vyhľadávania, ako neelektronické údaje.

111. Prehliadanie elektronických údajov bez možnosti zmeny alebo vymazania archivovaných elektronických záznamov, alebo kopírovanie v rámci počítačového

systému, alebo do iného počítačového systému, nepredstavuje „sprístupnenie“ záznamov. Iba situácia, keď existuje možnosť zmeniť, alebo vymazať archivované údaje, by mala byť považovaná za prístup, stiahnutie, „sprístupnenie“ alebo odstránenie záznamov a materiálov. Archivár musí byť schopný kontrolovať pridelenie prístupu k archivovaným elektronickým údajom „iba na čítanie“, aby bolo možné overiť, že požiadavky na archivované údaje sú plnené.

112. Elektronické údaje musia byť prístupné a čitateľné a ich integrita musí byť udržiavaná po celú dobu archivovania. Pokiaľ je zvolené hybridné riešenie (napr. paralelne sú udržiavané údaje „na papieri“ a elektronické údaje), vedenie testovacieho pracoviska musí špecifikovať, ktoré záznamy sú riadené, aby bolo archivovanie relevantné.

113. Elektronické archivovanie musí byť považované za nezávislý postup, ktorý musí byť primerane validovaný. Pri vypracovaní a validovaní postupu pre archivovanie musí byť uplatnené hodnotenie rizika. Príslušné hostované systémy, na ktorých sa budú dáta uchovávať a formát uchovávaných dát musí byť zhodnotený z pohľadu dostupnosti, čitateľnosti a vplyvu na integritu údajov po dobu archivovania. Pozornosť musí byť venovaná archivovaniu elektronických údajov v otvorenom formáte, ktorý je nezávislý od formátu súborov vlastníka, napr. výrobcu zariadenia. Tam, kde je potrebné konvertovanie údajov, platia požiadavky z článku 2.8. Archivár, ktorý má výlučnú zodpovednosť, môže delegovať úlohy týkajúce sa spravovania elektronických údajov na kvalifikovaných pracovníkov, alebo automatizované procesy (napr. kontrola prístupu). Pokiaľ ide o úlohy a zodpovednosti v procese archivovania, platí OECD GLP Advisory Document No. 15.

114. Musia byť implementované postupy, ktoré zabezpečia, že dlhodobá integrita údajov, uchovávaných v elektronickej forme nebude ohrozená. Pokiaľ sa v priebehu obdobia archivácie zmenia dátové médiá, fomát údajov, hardvér alebo softvér archivačného systému (nie systémov na zber údajov), vedenie testovacieho pracoviska sa musí ubezpečiť, že to negatívne neovplyvní dostupnosť, čitateľnosť a integritu archivovaných údajov. Musí byť zabezpečená a otestovaná trvalá schopnosť znovu získať/obnoviť údaje. Tam, kde sa predpokladajú problémy s dlhodobým prístupom k údajom, alebo kde musia byť počítačové systémy vyradené, musia byť zavedené postupy, ktoré zabezpečia nepretržitú čitateľnosť údajov. Toto môže byť, napríklad, vytlačenie údajov na papier, alebo konvertovanie údajov do iného formátu, alebo prenos údajov do iného systému. Pokiaľ je potrebná migrácia údajov, vrátane konvertovania do iného dátového formátu alebo vytlačenie údajov na papier, musia byť splnené požiadavky tejto smernice pre migráciu údajov. V prípade, že sú potrebné zmeny v archivačnom systéme, do úvahy sa ako relevantné štandardné postupy musia brať hodnotenie rizík, kontrola zmeny, riadenie konfigurácie a režim testovania. Nakoľko obsah a význam všetkých elektronických údajov musí byť v priebehu archivovania zachovaný, kompletný zoznam informácií musí byť identifikovaný a archivovaný (napr. primárne údaje, metadáta, potrebné na správne pochopenie významu záznamu, alebo na rekonštrukciu jeho zdroja, elektronické podpisy, audit trails, atď.).

115. Pokiaľ je elektronicky podpísaný záznam uchovávaný elektronicky, jeho integrita musí byť po celý čas uchovávania zabezpečená. Počas doby archivovania musí byť možná verifikácia integrity podpísaného záznamu, podporných metadát a elektronického

podpisu a musí byť hodnotená. Periodickosť hodnotenia musí byť vedením testovacieho pracoviska stanovená na základe hodnotenia rizika.

116. V správe zo štúdie musí vedúci štúdie identifikovať všetky so SLP súvisiace údaje, ktoré sú elektronicky archivované a umiestnenie elektronického archívu.

117. Akékoľvek údaje, uchovávané ako podporné pre relevantné počítačové systémy, ako zdrojový kód, údaje z vývoja, validácie, prevádzky, záznamy z údržby a monitorovania, musia byť tiež uchovávané minimálne tak dlho, ako záznamy zo štúdie, súvisiace s týmito systémami.

118. Žiadne elektronicky uchovávané údaje nesmú byť zničené bez súhlasu vedenia testovacieho pracoviska, a tam, kde je to aplikovateľné, bez povolenia objednávateľa a bez príslušnej dokumentácie.

5.3.12 Kontinuita činnosti a obnova systému po havárii

119. V prípade havárie systému musia byť prijaté opatrenia pre zabezpečenie kontinuity podpory počítačových systémov, ktoré sú používané v procesoch, súvisiacich so SLP (napr. manuálne zadávanie údajov, alebo alternatívny počítačový systém). Čas potrebný na zavedenie alternatívnych riešení musí byť založený na hodnotení rizika, ktoré musí byť primerané pre daný systém a obchodný proces, ktorý podporuje. Tieto náhradné riešenia musia byť primerane dokumentované a testované.

120. Musia byť zavedené postupy, opisujúce opatrenia, prijaté v prípade čiastočného, alebo úplného zlyhania počítačového systému. Opatrenia môžu byť v rozsahu od plánovanej výmeny hardvéru za iný náhradný, až po prechod späť k alternatívnemu systému. Všetky rezervné plány musia byť dobre dokumentované a validované a musia zabezpečiť nepretržitú integritu údajov a to, že štúdia nebude žiadnym spôsobom ohrozená. Pracovníci, podieľajúci sa na SLP, musia byť s náhradnými plánmi oboznámení.

121. Postupy pre obnovenie počítačového systému musia závisieť od kritickosti systému, ale dôležité je, aby originály, alebo záložné kópie všetkých softvérov, vo verziách relevantných pre validovaný počítačový systém, boli udržiavané, dostupné, alebo musia byť k dispozícii dohodou o servisných službách. Ak sa pri obnove zmení hardvér alebo softvér, musia sa opäť uplatniť požiadavky na validáciu podľa tejto smernice.

122. Keď sa použije alternatívny postup pre zber údajov, teda ak sú ručne zaznamenané údaje následne zadané do počítača, takýto postup musí byť jasne identifikovaný. Postup zadávania údajov musí byť validovaný a musí tam byť vyhlásenie, že tieto zadané údaje sú rovnocenné s ručne zaznamenanými primárnymi údajmi. Ručne zaznamenané primárne údaje musia byť uchovávané ako originálny záznam a záznamy musia byť archivované, počas obdobia, ako všetky ostatné záznamy. Alternatívne postupy zálohovania musia slúžiť na minimalizáciu rizika straty akýchkoľvek údajov a zabezpečiť, aby tieto alternatívne údaje ostali zachované.

5.4 FÁZA VYRADENIA

123. Vyradenie systému je tiež považované za fázu životného cyklu systému. Musí byť plánované, založené na hodnotení rizika a dokumentované. Pokiaľ je potrebná migrácia, alebo archivovanie údajov súvisiacich so SLP, riziká ohrozenia dát musia byť vylúčené a aplikujú sa požiadavky tejto smernice.

5.5 REFERENCIE

"Good Practices for Computerised Systems in Regulated GxP Environments" [platné od 25.09.2007] PIC/S PI 11-3

"Computerised Systems used in Nonclinical Safety Assessment: Current Concepts in Validation and Compliance" [vydané 2008, DIA, Red Apple II]."

"GAMP 5 - A Risk Based Approach to Compliant GxP Computerised Systems" ISPE Good Automated Manufacturing Practice © ISPE 2007

"Establishment and Control of Archives that Operate in Compliance with the Principles of GLP", [ENV/JM/MONO(2007)10], OECD GLP Podradný dokument č. 15.

The rules governing medicinal products in the European Union. Volume 4 - Guidelines for good manufacturing practices for medicinal products for human and veterinary use. Príloha 15 k EU Guide of GMP "Qualification and Validation" október 2015.

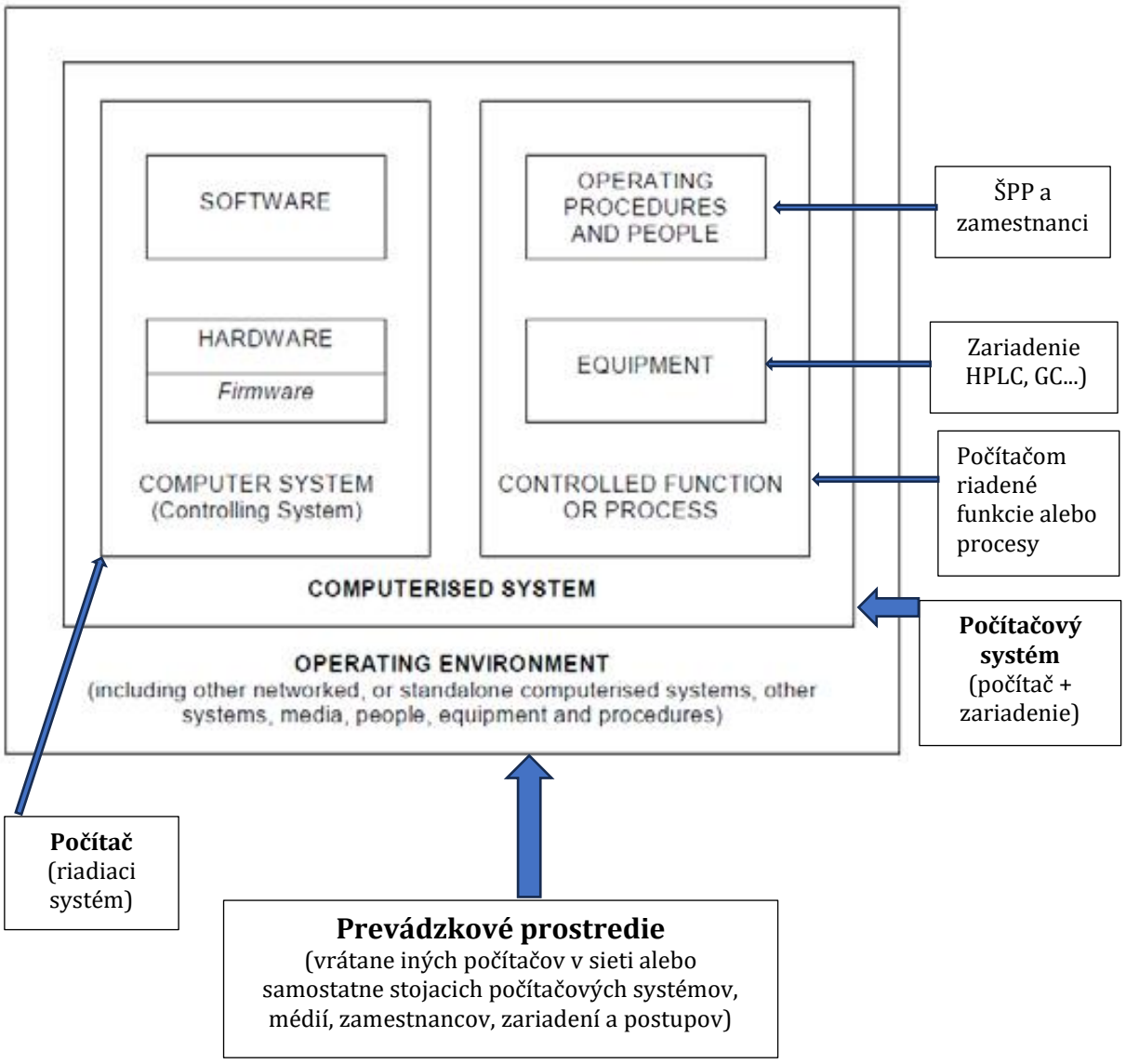
6 PRÍLOHY

6.1 PRÍLOHA 1: ÚLOHY A ZODPOVEDNOSTI

Úloha	Zodpovednosť
Majiteľ obchodného procesu	Jednotlivec alebo organizácia zodpovedná za zabezpečenie zdrojov pre obchodný proces (napr. predklinický pokus)
IT pracovníci	Pracovníci zaangažovaní do nákupu, inštalácie a údržby počítačového systému. Zodpovednosť zahŕňa napr. prevádzkovanie a údržbu hardvéru a softvéru, zálohovanie, riešenie problémov, atď.
Pracovníci	Všetky osoby, zaangažované vo validácii, prevádzke alebo podpore počítačového systému
Zabezpečenie kvality	(viď ENV/MC/CHEM(98)17 "OECD Principles of GLP", (1997), 2.2.8.)
Objednávateľ	(viď ENV/MC/CHEM(98)17 "OECD Principles of GLP", (1997), 2.2.5.)
Vedúci štúdie	(viď ENV/MC/CHEM(98)17 "OECD Principles of GLP", (1997), 2.2.6.)
Dodávateľ	Tretie strany, predávajúci, interné oddelenia IT, poskytovatelia služieb, vrátane poskytovateľov hostovaných služieb, atď.
Vlastník systému / vlastník IT	Jednotlivec, ktorý je zodpovedný za dostupnosť, podporu a údržbu systému a za bezpečnosť údajov v tomto systéme. Vlastník systému je zodpovedný za zabezpečenie toho, že počítačový systém je podporovaný a udržiavaný v súlade s aplikovateľnými postupmi. Vlastník systému koná v mene vedenia testovacieho pracoviska. Globálne systémy IT môžu mať globálnych vlastníkov systému a lokálnych vlastníkov systému, ktorí riadia miestnu implementáciu(viď GAMP 5).
Vedenie testovacieho pracoviska	(viď ENV/MC/CHEM(98)17 "OECD Principles of GLP", (1997), 2.2.3.)
Používateľ	Pracovníci, prevádzkujúci počítačový systém v štúdii SLP.
Vedúci validácie	Vymenovaná osoba, zodpovedná za projekt validácie

6.2 PRÍLOHA 2: GLOSÁR

Pojem	Definícia
Kritériá akceptácie	Dokumentované kritériá, ktoré musia byť splnené pre úspešné ukončenie fázy testovania alebo pre splnenie požiadaviek dodávky.
Akceptačné testovanie	Formálne testovanie počítačového systému v jeho plánovanom prevádzkovom prostredí za účelom stanovenia, či boli splnené všetky akceptačné kritériá a či je systém vhodný na pužitie.
Koncepcia prideľovania práv	Koncepcia prideľovania práv je formálny postup na definovanie a kontrolu prístupových práv a privilégií v počítačovom systéme.
Zálohovanie	Opatrenie, vykonané za účelom obnovy dátových súborov alebo softvéru, pre obnovenie spracovávania, alebo pre použitie alternatívneho počítačového zariadenia po zlyhaní alebo havárii systému.
Kontrolovanie zmeny	Sústavné hodnotenie a dokumentovanie prevádzky systému a zmien v ňom za účelom určenia, či je, po akejkoľvek zmene v počítačovom systéme, potrebná validácia.
Riadenie zmeny	Riadenie zmeny je proces kontrolovania životného cyklu zmien.
Komerčný off-the-shelf (COTS) produkt	Softvér alebo hardvér je komerčným off-the-shelf (COTS) produktom, pokiaľ je poskytnutý predávajúcim bežnej verejnosti, keď je k dispozícii v mnohých identických kópiách a keď je vedením testovacieho pracoviska implementovaný priamo, alebo s nejakým prispôsobením
Počítačový systém	"Počítačový systém je funkcia (proces, alebo postup), integrovaná s počítačom a vykonávaná zaškolenými pracovníkmi. Funkcia je riadená počítačovým systémom. Riadiaci počítačový systém pozostáva z hardvéru a softvéru. Funkcia riadenia pozostáva zo zariadenia ktoré je riadené a prevádzkových postupov, vykonávaných pracovníkmi. " *PIC/S PI 11-3 "Good Practices for Computerised Systems in Regulated GxP Environments"*



Konfigurácia	Konfigurácia je usporiadanie funkčných jednotiek a týka sa výberu hardvéru a softvéru a dokumentácie. Ovplyvňuje funkciu a výkonnosť systému.
Riadenie konfigurácie	Riadenie konfigurácie zahŕňa tie činnosti, ktoré sú potrebné na to, aby bolo možné presne definovať počítačový systém v určitom čase.
Riadená funkcia	Je proces alebo operácia, integrovaná do počítačového systému a vykonávaná zaškolenými ľuďmi.
Nápravné a preventívne opatrenia	Koncepcia nápravných a preventívnych opatrení sa zameriava na systematické skúmanie zásadných príčin identifikovaných

	problémov alebo rizík a úsilie o predchádzanie ich opätovnému výskytu.
Prispôsobený počítačový systém	Počítačový systém, individuálne prispôsobený tomu, aby vyhovoval konkrétnym procesom.
Údaje (odvodené údaje)	Odvodené údaje závisia od primárnych údajov a môžu byť zrekonštruované z primárnych údajov (napr. konečné koncentrácie, ako boli tabuľkovým procesorom vypočítané z primárnych údajov, výsledkové tabuľky sumarizované LIMSom, atď.).
Údaje (primárne údaje)	Údaje (primárne údaje) môžu byť definované ako merateľné alebo opisné atribúty fyzickej entity, procesu alebo udalosti. Zásady SLP definujú primárne údaje ako všetky laboratórne záznamy a dokumentáciu, vrátane údajov, priamo zadaných do počítača prostredníctvom automatického prístrojového rozhrania (prepojenia), ktoré sú výsledkom primárnych pozorovaní a činností v štúdii a ktoré sú potrebné pre rekonštrukciu a vyhodnotenie správy z tejto štúdie.
Schválenie údajov	Schválenie údajov znamená uzamknutie údajov po zbere, overení a napr. transformácii, aby boli tieto vhodné na použitie v záznamoch.
Zhromažďovanie údajov	Zhromažďovanie údajov sú činnosti, ktoré sa typicky vykonávajú pri plánovaní, zbere a overovaní údajov a súvisiacich metadát.
Migrácia údajov	Migrácia údajov je činnosť, napr. transport elektronických údajov z jedného počítačového systému do druhého, prenos údajov medzi pamäťovými médiami alebo jednoducho prechod údajov z jedného stavu do druhého [napr. konvertovanie údajov do iného formátu]. Pojem „údaje“ sa vzťahuje na „primárne údaje“, ako aj na “metadáta”.
Riadenie odchýlok	Riadenie odchýlok (incidentov) zahŕňa tie činnosti, ktoré umožnia identifikovanie, dokumentovanie, vyhodnotenie a pokiaľ je to vhodné, preskúmanie za účelom zistenia príčin, ktoré spôsobili odchýlku (incident) a predídenie jej opätovnému výskytu.
Elektronický záznam	Akákoľvek kombinácia textových, grafických, dátových, zvukových, obrazových alebo iných informácií v digitálnej forme, ktorá je vytvorená, modifikovaná, udržiavaná, archivovaná, obnovená, alebo distribuovaná počítačovým systémom.
Elektronický podpis	Elektronický spôsob, ktorým môže byť nahradený ručný podpis alebo iniciály, za účelom jednoznačného schválenia, povolenia alebo overenia konkrétnych dátových vstupov.

Hybridné riešenie záznamov (systém)	Súčasná existencia papierových a elektronických záznamov a podpisov. Príklady zahŕňajú kombinácie papierových (alebo iných neelektronických médií) a elektronických záznamov, papierových záznamov a elektronických podpisov, alebo ručných podpisov, spojených s elektronickými záznamami.
Životný cyklus	Prístup k vývoju počítačového systému, začínajúci identifikáciou požiadaviek používateľa, pokračujúci navrhnutím, integráciou, kvalifikáciou, validáciou zo strany požívateľa, kontrolou a údržbou a končiaci vtedy, keď je systém vyradený.
Model životného cyklu	Model životného cyklu opisuje fázy alebo činnosti projektu od koncepcie až po vyradenie produktu. Špecifikuje vzťah medzi fázami projektu, vrátane kritérií prechodu, mechanizmov spätnej väzby, míľnikov, východiskových bodov, preskúmaní a výstupov.
Metadáta	Metadáta sú údaje o údajoch. Metadáta sú všetky informácie, používané na identifikáciu, opis a vzťahy elektronických záznamov, alebo ich prvkov. Metadáta dávajú údajom význam, poskytujú kontext, definujú štruktúru a umožňujú spätné obnovenie v rámci systémov a použiteľnosť, autentickosť a auditovateľnosť v čase.
Operačný systém	Program alebo súhrn programov, ktoré riadia prevádzku počítača. Operačný systém môže poskytnúť služby, akými sú vyčlenenie zdrojov, plánovanie, kontrola vstupov/výstupov a riadenie údajov.
Periférne zariadenia	Všetky pripojené prístrojové zariadenia, alebo pomocné alebo vzdialené komponenty, ako sú tlačiarne, modemy, terminály, atď.
Proces	Proces je séria činností, určených na dosiahnutie konkrétneho výsledku. Proces definuje požadované činnosti a zodpovednosti pracovníkov, určených na vykonanie práce. Primerané nástroje a zariadenia, postupy a metódy definujú úlohy a vzťahy medzi úlohami.
Kvalifikácia	Činnosť na dokázanie toho, že všetky zariadenia, vrátane softvéru, fungujú správne a sú vhodné na svoj účel.
Uznané technické normy	Normy, ako sú zverejnené národnými, alebo medzinárodnými normotvornými orgánmi (ISO, IEEE, ANSI, atď.)
Regulované záznamy	Sú záznamy, ktorých udržiavanie alebo predkladanie je vyžadované predpismi SLP. Regulovaný záznam môže byť v rôznych formátoch, napr. elektronicky, na papieri, alebo obomi spôsobmi.

Riziko	Kombinácia pravdepodobnosti výskytu a závažnosti spôsobenej škody
Analýza rizík	Odhad rizika spojeného s identifikovaným nebezpečenstvom. Je to kvalitatívny alebo kvantitatívny proces prepájania pravdepodobnosti výskytu a závažnosti škôd.
Hodnotenie rizika	Hodnotenie rizika pozostáva z identifikácie nebezpečenstva, analýzy a hodnotenia rizika súvisiaceho s vystavením sa tomuto nebezpečenstvu. Za hodnotením rizika nasleduje kontrola rizika.
Kontrola rizika	Proces, prostredníctvom ktorého sú dosiahnuté rozhodnutia a implementované ochranné opatrenia na zníženie rizika, alebo udržanie rizika v rámci špecifických hraníc.
Identifikácia rizika	Systematické použitie informácií za účelom identifikovania nebezpečenstva, odvolávajúc sa na otázku rizika alebo opis problému. Informácia môže zahŕňať historické údaje, teoretické analýzy, informované názory a obavy zainteresovaných strán.
Riadenie rizika	Koncepcia riadenia rizika kvality je opísaná ako „systematický proces“ hodnotenia, kontroly, komunikácie a preskúmania rizika pre kvalitu.
Znižovanie rizika	Činnosti, vykonané za účelom zníženia pravdepodobnosti, že bude spôsobená škoda a závažnosti tejto škody.
Bezpečnosť	Ochrana počítačového hardvéru a softvéru pred náhodným, alebo svojvoľným vstupom, použitím, modifikáciou, zničením alebo odhalením. Bezpečnosť sa týka aj pracovníkov, údajov, komunikácií a fyzickej a logickej ochrany počítačových inštalácií
Softvér	Program, získaný alebo vyvinutý, adaptovaný, alebo vyrobený na mieru podľa požiadaviek testovacieho pracoviska za účelom riadenia procesov, zberu údajov, spracovania údajov, oznamovania údajov a/alebo archivovania.
Zdrojový kód	Originálny počítačový program vyjadrený v pre ľudí čitateľnej forme (programovací jazyk), ktorý musí byť preložený do strojom čitateľnej formy pred tým, ako môže byť vykonaný počítačom.
Špecifikácia požiadaviek používateľa	Špecifikácia požiadaviek používateľa definuje v písomnej forme, čo používateľ očakáva, že počítačový systém bude schopný robiť.
Preskúmanie používateľa (User review)	Preskúmanie prístupových práv a privilégií používateľa.

Validácia	Činnosť zabezpečujúca, že proces vedie k očakávaným výsledkom. Validácia počítačového systému vyžaduje zabezpečenie a preukázanie vhodnosti na svoj účel
Validačná stratégia	Validačná stratégia definuje v dokumente proces a všetky činnosti, súvisiace s jednotlivými fázami validácie počítačového systému.

Ďalšie definície pojmov je možné nájsť v "*OECD Principles of Good Laboratory Practice.*"

***