**Příloha č. 7**

**Struktura a rozsah provozní dokumentace informačních systémů – požadavky TSK na zpracovatele dokumentace**

**v. 1.0**

**1. Úvod**

* určení/specifikace oprávněných osob pro práci s provozní dokumentací
* použité zkratky
* základní popis informačního systému (HW, SW, služby, procesy ad.)

**2. Popis informačního systému**

* úplný a přesný popis informačního systému doplněný schématem, architektura systému
* přesné umístění informačního systému (lokalita, objekt, místnosti)
* důvěrnost dat a informací zpracovávaných informačním systémem (rozdělení do čtyř úrovní dle NÚKIB), OÚ dle GDPR a uvedení rozsahu/objemu dat v každé kategorii
* soulad s GDPR a další legislativou (Zákon o kybernetické bezpečnosti ad.)
* předpokládaný počet uživatelů (interních i externích), licence k informačnímu systému a případná omezení v právech užívání
* vztah k jiným informačním systémům TSK a systémům dalších subjektů
* zdůvodnění použití kryptografických prostředků

**2.1. HW konfigurace informačního systému**

* Úplný a přesný seznam HW komponent včetně sériových čísel.

U samostatných počítačů (1 a více):

* typ PC s bližšími údaji o jeho komponentách včetně HDD,
* typ monitoru včetně typu připojení k PC (VGA, DVI apod.)
* human interface (klávesnice, myš) včetně typu připojení (PS2, USB apod.)
* HW kryptografické prostředky
* periferní zařízení (např. zálohování, UPS)

Informační systém typu LAN:

* servery – typ a bližší údaje o jejich komponentách
* pracovní stanice – typ a bližší údaje o jejich komponentách včetně lokálních periferních zařízeních (např. tiskárny, UPS)
* HW kryptografické prostředky
* síťové periferní zařízení (např. síťové tiskárny, disková pole, zálohovací zařízení, centrální UPS)
* pasivní prvky síťové infrastruktury (datové rozvody) – typ, způsob vedení apod.
* aktivní prvky síťové infrastruktury (např. router, switch)

**2.2. SW konfigurace informačního systému**

* Úplný a přesný seznam SW komponent včetně označení jejich verzí

SW komponenty jsou zejména:

* operační systémy
* aplikační SW (komerční i speciální),
* antivirové programy
* SW kryptografické prostředky
* zálohovací utility
* administrátorské utility

U aplikací dále specifikujte:

* architekturu aplikací, jejich začlenění v informačním systému
* moduly a funkcionality
* datový model
* rozhraní aplikací

**3. Personální bezpečnost**

* definice rolí působících v informačním systému (podle bezpečnostní politiky)
* seznam konkrétních požadavků na osoby v jednotlivých rolích informačního systému
* popis postupu pro zařazení/vyřazení uživatele do/z informačního systému

**4. Počítačová bezpečnost**

Pro nasazené systémy uvést původ použitého bezpečnostního nastavení (dodané TSK, vlastní návrh, dodané třetí stranou apod.)

**4.1. Jednoznačná identifikace a autentizace**

* popis nastavení bezpečnostních parametrů informačního systému, integrace do AD, IdM apod.
* popis případných použitých speciálních prostředků pro identifikaci a autentizaci včetně konkrétních údajů a nastavení (smart card, biometrická zařízení, apod.)
* pokud je používána identifikace a autentizace na aplikační úrovni, tak popsat a specifikovat potřebné nastavení
* definice povinnosti uzamčením pracovní stanice nebo samostatného osobního počítače při krátkodobém opuštění zapnutého počítače a umožněním opětovné práce v systému až po úspěšné identifikaci a autentizaci uživatele
* definice povinnosti bezpečného ukládání hesel pro speciální účty ve stanoveném úschovném objektu (vestavěné účty administrátorů, účty důležitých služeb, BIOS apod.)

**4.2. Volitelné řízení přístupu**

* pokud je používáno na aplikační úrovni, popsat a specifikovat potřebné nastavení
* matice přístupových práv pro uživatele
* způsob a rozsah nakládání s daty mimo perimetr TSK (lze/nelze předávat a za jakých podmínek)

**4.3. Auditní záznamy a monitoring**

* popis nastavení bezpečnostních parametrů informačního systému
* definice povinnosti bezpečnostního správce (četnost a rozsah prověřování auditních záznamů, délka uchovávání)
* definovat omezení přístupu uživatelů k auditním záznamům
* uvést a popsat používané nástroje pro analýzu auditních záznamů
* uvést a popsat používané nástroje monitoringu dat a jednotlivých částí informačního systému (HW i SW komponenty)

**4.4. Ochrana před škodlivým kódem**

* uvést typ antivirového prostředku
* definovat, kdo bude zajišťovat jeho aktualizaci
* definovat, jak často bude prováděna jeho aktualizace

**4.5. Instalace, používání a bezpečnostní nastavení SW**

* uvést způsob zajištění správy konfigurace a vedení seznamu SW bezpečnostním správcem, včetně údaje o případně používaném SW nástroji
* uvést způsob zajištění údržby SW (aplikace opravných programových balíčků a aktualizací vydávaných výrobci SW)

**4.6. Komunikační bezpečnost LAN**

Uvést kompletní údaje o LAN:

* typ kabeláže a použité standardy
* síťové protokoly a pro ně potřebná konfigurace (např. MAC adresy, IP adresy a masky podsítí pro IP protokol)
* topografie LAN (fyzické umístění jednotlivých zařízení - servery, pracovní stanice, aktivní prvky sítě, kryptografické prostředky, kabely)
* topologie LAN (např. sběrnicová, hvězdicová, kruhová, fyzická segmentace na jednotlivých vrstvách OSI modelu a skutečná konfigurace síťových komponent, případně logická segmentace na bázi VLAN a konfigurační soubory)

**4.7. Servisní činnost**

* definovat povinnosti pracovníků správy systému (platné i pro externí pracovníky) při provádění nebo zajišťování servisní činnost (kdo, jak a kde může servis provádět)
* definovat podmínky pro náhradní HW komponenty používané při servisu
* definovat podmínky provádění servisu s ohledem na ochranu dat a informací (vyjímaní nosičů informací apod.)
* definovat povinnost používat v informačním systému pouze SW a HW vybavení odpovídající bezpečnostním požadavkům

**4.8. Požadavky na dostupnost**

* uvést požadavky na dostupnost informačního systému jako celku + podrobně pro všechny klíčové kritické části informačního systému
* definovat systém zálohování SW i HW prostředků pro zajištění dostupnosti informačního systému
* definovat systém a rozsah archivace dat
* definovat a popsat minimální funkčnost systému, která musí být zajištěna
* definovat a popsat způsob obnovy systému
* definovat odpovědnosti za zálohování a obnovu systému

**5. Kryptografická ochrana**

Uvést jaký kryptografický prostředek bude v informačním systému používán, přesný typ a počty prostředků, jak bude zajišťována správa klíčů a certifikátů, kde budou umístěny a jak bude zajištěna jejich bezpečnost a zabezpečení (i fyzické)

**6. Řízení a plánování kontinuity**

* definovat typy a modelové způsoby řešení možných krizových situací vč. exit strategy
* definovat typy a modelové způsoby řešení bezpečnostních incidentů
* definovat typy a modelové způsoby řešení možné kompromitace (v případě použití kryptografické ochrany)
* definovat povinnosti pracovníků – standardní provozní procedury a pravidelné činnosti
* definovat povinnost pracovníků správy systému při řízení změn v provozovaném informačním systému (jak změny provádět, jak změny hlásit TSK, jak je začlenit do aktuální dokumentace informačního systému)
* definovat povinnost pracovníků správy systému při provádění testů bezpečnosti (způsob provádění a vyhodnocování testů)

**7. Dokumentace**

* uživatelská dokumentace
* administrátorská dokumentace
* jiná dokumentace (produktová dokumentace atd…)