# Návod na vyplnenie

šablóny bezpečnostného projektu informačných systémov.

# OBSAH

# 1. Úvod

Zákon č. 122/2013 Z. z. o ochrane osobných údajov stanovuje pre prevádzkovateľov informačných systémov s osobnými údajmi povinnosť vypracovania bezpečnostného projektu. Zákon č. 122/2013 Z. z. o ochrane osobných údajov (ďalej len zákon) zároveň svojím uvedením do platnosti ruší pôvodný zákon č. 428/2002 Z. z. o ochrane osobných údajov.

Tento dokument je doplnkom sady súborov Šablóny bezpečnostného projektu (ďalej len projektová šablóna). Dokument udáva a rozširuje metodické pokyny uvedené v projektovej šablóne.

## 1.1 Dokumenty šablony

Dodávané dokumenty sú primárne spracované v balíku Microsoft Word. Pre ich lepšiu dostupnosť boli konvertované aj do formátov Portable Document Format (.pdf), OpenDocument (.odt).

Súbory šablony sú uložené v nasledujúcej adresárovej štruktúre:

BPIS:

## 1.2 Popis súborov projektu

V adresári **1-projekt** sa nachádzajú súbory samotnej šablóny bezpečnostného projektu, ktoré je potrebné prispôsobiť pre konkrétne prevádzkové podmienky spoločnosti:

**P1-Politika**
Deklaratívny dokument. V jeho obsahu nie je potrebné robiť zmeny väčšieho rozsahu, pokiaľ prevádzkovateľ v zásadnej miere nechce zmeniť rozsah a formu štandardnej navrhovanej politiky bezpečnosti organizácie.

**P2-Projekt**
Hlavný dokument projektu, kde sa spravidla najviac modifikuje obsah. Vyplňuje sa podľa priložených inštrukcií v samotnom texte. Výsledkom úprav je dokument **„Bezpečnostný projekt informačných systémov“**. Pomôckou k vykonaniu analýzy v rámci bezpečnostného projektu je súbor v adresári **1-projekt/dotazniky** s názvom **D1-analyza_bezpecnosti**, ktorý pomôže na základe sady otázok stanoviť riziká.

**P3-Smernice**
Navrhované znenie obsahu bezpečnostných smerníc. Bezpečnostné smernice sú syntetickou časťou bezpečnostného projektu. Budú súhrnom všetkých navrhovaných opatrení projektu z jeho kapitoly **„Analýza bezpečnosti“**.

V tomto dokumente sú potrebné zmeny, pokiaľ prevádzkovateľ chce realizovať opatrenia nad rámec návrhu alebo naopak spraviť ich benevolentnejšie. Ustanovenia smerníc by mali vždy odrážať navrhované opatrenia z bezpečnostného projektu.

**P4-Prílohy**
Prílohy k projektu, napr. preukázanie zhody. Je potrebné modifikovať podľa potreby.

V podadresári **1-projekt/dokumenty** sa nachádzajú vzory formulárov a dokumentov s pridanou hodnotou. Pre vypracovanie bezpečnostného projektu nie sú nevyhnutné, ich použitie môže vyplynúť z konkrétnych potrieb prevádzkovateľa.

# 2. Informácie

Pre zjednodušenie a sprehľadnenie práce pri vypracúvaní projektu z dodávanej šablóny boli dôležité informácie, pokyny a príklady priamo vpísané do dokumentov projektovej šablóny a farebne zvýraznené podľa nasledujúcich vzorov. K úprave môžete použiť priamo projektové súbory šablony (formát DOCX, DOC alebo ODT) alebo začať tvoriť vlastný dokument podľa predlohy šablóny (kopírovaním).

Pomôckou k vykonaniu analýzy v rámci bezpečnostného projektu je súbor uložený v adresári **1-projekt/dotazniky** s názvom **D1-analyza_bezpecnosti**, ktorý pomôže na základe sady otázok stanoviť bezpečnostné riziká.

Riaďte sa, prosím, týmito návodmi a pokynmi, ktoré sú uvádzané v priebehu textov súborov šablóny bezpečnostného projektu.

**Pokyny:** Text označený v dokumente takýmto štýlom (zvýraznený červenou farbou) uvádza pokyny a inštrukcie na vyplnenie danej časti dokumentu. Vo výslednom bezpečnostnom projekte je ho potrebné odstrániť.

**Príklad:** Text uvádzaný v dokumente takýmto spôsobom (zvýraznený modrou farbou) uvádza príklad použitia konkrétnych údajov. Vo výslednom bezpečnostnom projekte je ho potrebné nahradiť skutočnými požadovanými informáciami alebo modifikovať pre konkrétne použitie.

**Informácia:** Text uvádzaný v dokumente takýmto spôsobom (zvýraznený žltou farbou) uvádza doplňujúce a rozširujúce informácie pre vypracovanie danej časti. Vo výslednom bezpečnostnom projekte je ho možné vynechať, alebo podľa potreby použiť ako doplňujúcu informáciu.

Texty označované červenou farbou pre pokyny je potrebné z výsledného dokumentu odstrániť.

Farebné zvýraznenie pre príklady a informácie, ak budú ponechané vo výslednom dokumente, odstránite hromadne modifikáciou/zmazaním štýlu s názvom **„_exam_paragr“**, **„_exam_char“** a **„_info_paragr“**, **„_info_char“**.

Odporúčame vytvárané dokumenty verziovať pre možnosť vrátiť sa k predchádzajúcej verzii textu. Pre verziovanie použite prostriedky aplikácie editoru (napr. sledovanie zmien vo Worde) alebo vytvorte kópiu súboru, kde k názvu pridáte číslo verzie súboru.

## 2.1 Autorský zákon

Šablóna bezpečnostného projektu je dielom, a preto dodržujte, prosím, ustanovenia týkajúce sa autorského zákona uvedené v dodávaných dokumentoch. Porušenie autorských práv je trestné!

# 3. Podklady

Kapitola má za cieľ pomôcť identifikovať nevyhnutné informácie, podklady a materiály prevádzkovateľa potrebné k implementácii bezpečnostného projektu.

K realizácii bezpečnostného projektu je potrebné:

- doložiť informácie potrebné pre identifikovanie prevádzkovateľa (podľa položiek v projektovej šablóne)
  - informácie zo zriaďovacej listiny, obchodného alebo živnostenského registra
- podklady k informačným systémom
  - dokumentácia k softvérovým IS
  - používateľské príručky, návody
  - zoznam poverených používateľov IS
- popis okolia informačných systémov
  - zabezpečenie budov, kancelárií, verejných priestorov
  - kontrola prístupov do priestorov
  - orientačné plány priestorov
  - topológia počítačovej siete
  - miestnosti so servermi a ich zabezpečenie
  - realizácia a zabezpečenie pripojenia k Internetu
- technické zabezpečenie
  - zabezpečenie aktívnych sieťových prvkov (switch, firewall, router)
  - zabezpečenie pasívnych sieťových prvkov (vedenie, zásuvky)
- určiť právny základ informačného systému
  - personalistika – evidencia zamestnancov a ich pracovných zmlúv na základe príslušného zákona
  - prípadne pre ďalšie prevádzkované systémy
- zmluvy s tretími stranami
  - s dodávateľmi informačných systémov
  - so sprostredkovateľmi spracúvania osobných údajov
  - so spoločnosťami poskytujúcimi služby ohľadom informačných systémov alebo servisu hardvéru

# 4. Informačné systémy

Určenie relevantných informačných systémov, ktorých sa bude týkať spracovanie, je kľúčovou úlohou pri plánovaní samotného bezpečnostného projektu.

Pritom kritérium na posúdenie je jednoduché - informačný systém musí spracúvať osobné údaje. Pre zjednodušený pohľad sú to napr. meno, priezvisko, adresa, rodné číslo, číslo občianskeho preukazu.

**Osobný údaj**
Osobnými údajmi sú údaje týkajúce sa určenej alebo určiteľnej fyzickej osoby, pričom takou osobou je osoba, ktorú možno určiť priamo alebo nepriamo, najmä na základe

všeobecne použiteľného identifikátora alebo na základe jednej či viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú, fyziologickú, psychickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu.

**Spracovávanie osobných údajov**

Spracovávaním osobných údajov je vykonávanie akýchkoľvek operácií alebo súboru operácií s osobnými údajmi, napr. ich získavanie, zhromažďovanie, zaznamenávanie, usporadúvanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, premiestňovanie, využívanie, uchovávanie, likvidácia, ich prenos, poskytovanie, sprístupňovanie alebo zverejňovanie.

**Príklady systémov s osobnými údajmi:**

- personalistika a mzdy - PaM
  - elektronické aj papierové zoznamy
- korešpondencia
  - adresár, došlá/vyšlá pošta
- evidencia klientov, zákazníkov – fyzických osôb
- evidencia brigádnikov
- evidencia akcionárov, podielnikov, majiteľov
- evidencia ubytovaných (firemné ubytovacie zariadenie)
- napr. pre evidencie MsÚ
  - matričná evidencia/evidencia obyvateľov
  - evidencia plateného parkovania (parkovacie karty na meno)
  - opatrovateľská služba
  - agenda stavebného úradu
  - agenda záujmovo-umeleckej činnosti
  - databáza čitateľov Mestskej knižnice

# 5. Dôležité oblasti

Oblasti, ktorým treba venovať zvláštnu pozornosť, a ktorým sa podrobne zaoberá šablóna bezpečnostného projektu.

## 5.1 Informačné aktíva

Identifikácia a popis informačných aktív.

Zverejňovanie osobných údajov.

Poskytovanie osobných údajov.

Prenos osobných údajov do tretích krajín.

## 5.2 Pripojenie do Internetu

Pripojenie lokálnej siete do Internetu.

Využívanie služieb Internetu (web server, email server).

## 5.3 Písomnosti a tlačové výstupy

Vytváranie a skartácia tlačových zostáv a dokumentov s osobnými údajmi.

Prístupy k zariadeniam umožňujúcim reprodukciu materiálov.

Korešpondencia, adresáre (ukladanie, zabezpečenie).

## 5.4 Zálohovanie a archivácia

Postupy archivácie a zálohovania.

Organizácia a správa záložných a archívnych médií.

Zodpovednosti a poverenia za vytvárania záloh a archívov.

Uloženie aktívnych médií.

Skartácia médií po splnení účelu spracovania.

## 5.5 Fyzické aktíva

Počítačová sieť, rozmiestnenie prvkov, zabezpečenie.

Fyzické zabezpečenie serverov.

Zabezpečenie a konfigurácia klientských staníc.

Zabezpečenie komunikačných zariadení (modemy, faxy).

Elektronický dochádzkový systém.

Kontrola inštalovaných programov z hľadiska legálnosti a nebezpečnosti.

Zabezpečenie skríň, miestností.

Kontrola a preverovania zámkov, Prideľovanie a evidencia kľúčov.

Prideľovanie technických prostriedkov zamestnancom.

Antivírová ochrana.

Štandardizované postupy riešení porúch fyzických aktív.

## 5.6 Softvérové aktíva

Operačné systémy, ich bezpečnosť.

Evidencia inštalovaného softvéru.

Databázové systémy, ich popis, správa, údržba a zabezpečenie.

Bezpečnostné certifikáty od dodávateľov IS.

## 5.7 Personálne a organizačné opatrenia

Zakotvenie zodpovednosti v pracovných zmluvách a náplniach.

Školenia zamestnancov.

Kontroly a previerky zamestnancov.

Riešenie porušení nariadení a opatrení.

Postupy a dokumentovanie zavádzania a rušenia používateľských prístupov.

Postupy a forma prideľovania technických prostriedkov.

Dokumentovaný a kontrolovateľný schvaľovací proces pre zavádzanie nových informačných a evidenčných systémov

Bezpečnostné audity IS.

Bezpečnosť pri prístupe tretích strán.

Spolu súčinnosť s pobočkami.

## 5.8 Informačné systémy

Súhlas dotknutých osôb pre spracúvanie osobných údajov.

Popis jednotlivých častí IS, ich umiestnenie a zabezpečenie.

Registrácia informačných systémov.

Identifikovateľnosť prístupov a akcií používateľov.

Kontrola zaznamenaných prístupov a akcií používateľov.

Návrhy opatrení.