**Vzorová smernica o riadení dodávateľských vzťahov**



# Základné ustanovenie

Tento interný riadiaci akt definuje pravidlá pre riadenie dodávateľských vzťahov vrátane akvizícií a vývoja zo strany tretích strán v prostredí Organizácie.

Tento interný riadiaci akt je pre Organizáciu záväzný.

Všetci zamestnanci Organizácie a tretích strán sú povinní preukázateľne sa oboznámiť so znením
tohto dokumentu.

Tento interný riadiaci akt je spracovaný v kontexte:

a) Zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti,

b) Vyhlášky NBÚ č. 362/2018, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení,

c) Zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov,

d) Vyhlášky Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020, ktorou
sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy,

e) medzinárodnej normy ISO/IEC 27001 a ISO/IEC 27002.

# Riadenie dodávateľských vzťahov

Nasledujúce princípy riadenia dodávateľských vzťahov a služieb musia byť uplatňované minimálne vo vzťahu s dodávateľmi a tretími stranami, ktorých **činnosti priamo súvisia** alebo môžu mať vplyv na dostupnosť, dôvernosť a integritu prevádzky sietí a informačných systémov Organizácie ako prevádzkovateľa základnej služby.

Za identifikáciu dodávateľov priamo podporujúcich prevádzku základnej služby zodpovedá manažér kybernetickej bezpečnosti.

S týmito dodávateľmi musí byť uzatvorená zmluva o plnení bezpečnostných opatrení a plnení notifikačných povinností v zmysle zákona [č. 69/2018 Z.z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2021/287/20210801) o Kybernetickej bezpečnosti a vyhlášky [č. 362/2018 Z.z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/362/20190101#paragraf-8) o bezpečnostných opatreniach.

Povinnosť uzatvoriť zmluvu v zmysle tohto bodu neplatí, ak je dodávateľ prevádzkovateľom základnej služby, poskytovateľom digitálnej služby alebo ak je riziko vo vzťahu k činnosti, ktorá priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov Organizácie prostredníctvom tohto dodávateľa nízke.

V rámci riadenia dodávateľských služieb a akvizície informačných systémov sa pred uzatvorením zmluvy s treťou stranou **analyzujú riziká** dodávateľských služieb, akvizície, vývoja alebo údržby informačných systémov spôsobom popísaným v politike Riadenie bezpečnostných rizík. Táto analýza sa vykonáva ešte pred uzatvorením zmluvy
s dodávateľom.

***Pozn.:***

[**Metodika analýzy rizík**](https://www.nbu.gov.sk/wp-content/uploads/2021/12/Metodika_analyza_rizik_v1.0_12_2021.pdf) pre uplatnenie v procesoch riadenia rizika v zmysle požiadaviek zákona [č. 69/2018 Z.z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2021/287/20210801) o kybernetickej bezpečnosti a taktiež zákona č. [95/2019 Z.z.](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2019/95/20210801.html) o ITVS je podrobne spracovaná v materiály, publikovanom Národným bezpečnostným úradom [**na**](https://www.nbu.gov.sk/wp-content/uploads/2021/12/Metodika_analyza_rizik_v1.0_12_2021.pdf)[**tomto**](https://www.nbu.gov.sk/wp-content/uploads/2021/12/Metodika_analyza_rizik_v1.0_12_2021.pdf) **mieste**.

Za riadenie procesu posudzovania rizík spojených s dodávateľom a vyhotovenie analýzy bezpečnostných rizík zodpovedá manažér kybernetickej bezpečnosti.

Dodávateľ alebo tretia strana musí prehlásiť znalosť a schopnosť implementovať požadované bezpečnostné opatrenia, ktoré musia byť uvedené aj v zadaní a dokumentácii navrhovaného riešenia a zároveň musia byť súčasťou akceptačného testovania dodávaného riešenia, prípadne priamo vychádzajú z platnej legislatívy.

Pre **riadenie vzťahov** s tretími stranami:

• požiadavky na nový informačný systém alebo na rozšírenie / zmenu existujúceho systému musia obsahovať
aj požiadavky na bezpečnostné opatrenia,

• musí byť zaistené, že bezpečnostné opatrenia definované v zmluve s dodávateľmi sú implementované a dodržiavané.

**Monitorovanie poskytovaných služieb** musí zabezpečiť preukázateľné dodržiavanie dohodnutých bezpečnostných opatrení. Rozsah monitorovania a proces monitorovania musí preukázať:

• výkonnostné a kvalitatívne parametre poskytovaných služieb,

• poskytovanie informácií o bezpečnostných incidentoch a spôsob správy bezpečnostných incidentov,

• spôsob zaznamenávania záznamov pre audit, procesy vyhodnocovania a kontroly záznamov pre audit, bezpečnostných udalostí a prevádzkových problémov,

• spôsob riešenia iných problémov.

**Zmeny** v poskytovaní služieb, vrátane udržovania a zlepšovania existujúcich bezpečnostných politík, postupov
a bezpečnostných opatrení sa riadia s ohľadom na kritickosť systémov a procesov Organizácie, ktoré sú súčasťou opakovaného hodnotenia rizík.

Proces riadenia zmien služieb poskytovaných dodávateľmi by mal zohľadniť nutné zmeny vykonané zamestnancami Organizácie i nutné zmeny služieb poskytovaných dodávateľmi.

Pri všetkých zmenách a aktualizáciách bude uplatňované štandardné zmenové konanie.

# Zmluvy s tretími stranami

Zmluva s treťou stranou obsahuje najmenej:

* obdobie trvania zmluvy,
* ustanovenie záväzku tretej strany dodržiavať bezpečnostné politiky prevádzkovateľa základnej služby
a vyjadrenie súhlasu s nimi,
* ustanovenie o povinnosti chrániť všetky informácie poskytnuté prevádzkovateľom základnej služby tretej strane,
* ustanovenie o povinnosti dodržiavať a prijímať bezpečnostné opatrenia treťou stranou, konkrétnu špecifikáciu a rozsah bezpečnostných opatrení, ktoré prijíma tretia strana a vyjadrenie súhlasu s nimi,
* konkrétny rozsah činnosti tretej strany,
* zoznam pracovných rolí tretej strany, ktoré majú mať prístup k informáciám a údajom prevádzkovateľa základnej služby, s povinnosťou oznámiť prevádzkovateľovi základnej služby každú zmenu
v personálnom obsadení; osoba zúčastnená na predmete plnenia podpisuje vyjadrenie o zachovávaní mlčanlivosti,
* ustanovenie o rozsahu, spôsobe a možnosti vykonávania kontrolných činností a auditu prevádzkovateľom základnej služby v tretej strane,
* vymedzenie podmienok a možnosti zapojenia ďalšieho dodávateľa úplne alebo čiastočne zabezpečujúceho plnenie pre prevádzkovateľa základnej služby namiesto dodávateľa,
* ustanovenia o povinnosti informovať prevádzkovateľa základnej služby o kybernetickom bezpečnostnom incidente a o všetkých skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti,
* ustanovenia o spôsobe a forme hlásenia ďalších informácií požadovaných prevádzkovateľom základnej služby na plnenie jeho povinností vyplývajúcich zo zákona a ich vymedzenie,
* ustanovenie o spôsobe a forme hlásenia všetkých informácií majúcich vplyv na zmluvu,
* ustanovenie o sankčných mechanizmoch pri porušení zmluvy,
* ustanovenia o podmienkach a spôsobe ukončenia zmluvy,
* záväzok tretej strany po ukončení zmluvného vzťahu vrátiť, previesť alebo aj zničiť všetky informácie, ku ktorým má tretia strana počas trvania zmluvného vzťahu prístup, prevádzkovateľovi základnej služby,
* záväzok tretej strany po ukončení zmluvného vzťahu udeliť, poskytnúť, previesť alebo postúpiť všetky potrebné licencie, práva alebo súhlasy nevyhnutné na zabezpečenie kontinuity prevádzkovanej základnej služby na prevádzkovateľa základnej služby; tento záväzok tretej strany stáva v platnosti
aj po ukončení zmluvného vzťahu po dobu dohodnutú zmluvnými stranami, ktorá nesmie byť kratšia ako päť rokov po ukončení zmluvného vzťahu

Zmluva uzatvorená s treťou stranou obsahuje **minimálne bezpečnostné opatrenia** pre oblasť:

* technických zraniteľností systémov a zariadení,
* riadenia bezpečnosti sietí a informačných systémov,
* riadenia prístupov,
* riešenia kybernetických bezpečnostných incidentov,
* monitorovania, testovania bezpečnosti a bezpečnostných auditov.

Organizácia vedie evidenciu všetkých uzatvorených zmlúv s tretími stranami a táto evidencia je súčasťou bezpečnostnej dokumentácie.

# Audit a kontrolné činnosti

Za výkon kontrolných činností a audit plnenia bezpečnostných opatrení treťou stranou zodpovedá manažér kybernetickej bezpečnosti.

Kontrolná činnosť sa vykonáva aspoň 1 krát za 2 roky u každého dodávateľa, alebo po identifikovaní závažného bezpečnostného incidentu v súvise s výkonom činností dodávaných treťou stranou najneskôr do 3 mesiacov od odhalenia takéhoto incidentu.

# Zmluva o podpore prevádzky, údržbe a rozvoji informačného systému (SLA - service level agreement)

SLA popisuje IT službu, dokumentuje **cieľovú úroveň služieb** a špecifikuje zodpovednosti poskytovateľa IT služby a Organizácie. Jej cieľom je definovať štandardy pre ponuku, ciele, zmluvné záležitosti, podporu a čokoľvek iné, čo sa týka ponúkaných služieb.

Jedná sa o komplexný dokument, ktorý Organizácia musí pravidelne kontrolovať, aby sa zabezpečila jeho aktualizácia.

SLA garantuje tretej strane a Organizácii dodržiavanie dohodnutých služieb. Tento dokument vymenúva všetky povinnosti oboch strán počas obchodného vzťahu.

Pre prípad potreby uzavretia s dodávateľom aj zmluvu SLA je možné použiť predpripravený vzor, ktorý je možné upraviť podľa požiadaviek Organizácie. [Vzor SLA zmluvy](https://www.mirri.gov.sk/wp-content/uploads/2021/01/VZOR_ZMLUVA_SLA_v012020.docx) je zverejnený na [web stránke MIRRI](https://www.mirri.gov.sk/sekcie/informatizacia/riadenie-kvality-qa/riadenie-kvality-qa/), kde sa nachádza aj vzorová [zmluva o dielo](https://www.mirri.gov.sk/wp-content/uploads/2022/02/VZOR_ZMLUVA_ZoD_Zmluva_o_dielo_v01_2022_public.docx).