

## **VNÚTORNÝ PREDPIS č. 4/2025**

# **SMERNICA O RIADENÍ TRETÍCH STRÁN V OBLASTI KYBERNETICKEJ BEZPEČNOSTI SLOVENSKEJ AKREDITAČNEJ AGENTÚRY PRE VYSOKÉ ŠKOLSTVO**

**V Bratislave 4. september 2025**

# SMERNICA O RIADENÍ TRETÍCH STRÁN V OBLASTI KYBERNETICKEJ BEZPEČNOSTI SLOVENSKEJ AKREDITAČNEJ AGENTÚRY PRE VYSOKÉ ŠKOLSTVO

Výkonná rada Slovenskej akreditačnej agentúry pre vysoké školstvo (ďalej len „výkonná rada“ a „agentúra“ alebo „SAAVŠ“) schválila dňa 4. septembra 2025 podľa § 7 ods. 10 písm. d) zákona č. 269/2018 Z. z. o zabezpečovaní kvality vysokoškolského vzdelávania a o zmene a doplnení zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon“) túto *Smernicu o riadení tretích strán v oblasti kybernetickej bezpečnosti SAAVŠ*.

## Článok 1 Úvodné ustanovenia

1. Riadenie tretích strán predstavuje postupy a vzťahy s tretími stranami, ktoré môžu mať alebo majú vplyv na kybernetickú a informačnú bezpečnosť v agentúre, pričom *tretiou stranou* sa rozumie najmä dodávateľ, príp. iná osoba, s ktorou agentúra vstupuje do zmluvného vzťahu. Všetky ustanovenia tejto smernice používajúce pojem „dodávateľ“ sa primerane uplatňujú na všetky tretie strany. Cieľom je upraviť proces riadenia dodávateľov agentúry a ich dodávok (služieb aj tovarov) a určiť za agentúru zodpovedné osoby.
2. Vnútorný predpis č. 2/2024 o bezpečnostnej stratégii kybernetickej bezpečnosti SAAVŠ a vnútorný predpis č. 3/2024 o metodike analýzy rizík informačnej bezpečnosti SAAVŠ vo vzťahoch s tretími stranami definuje základné zodpovednosti, pravidlá a zásady riadenia vzťahov s tretími stranami prostredníctvom zmlúv agentúry vrátane určenia jednotlivých legislatívnych požiadaviek kladených na dodávateľov a iné tretie strany.
3. Ustanovenia tejto smernice sa použijú v prípade, ak tretia strana má alebo by mohla mať vplyv na informačnú alebo kybernetickú bezpečnosť agentúry, najmä ak ide o dodávateľa podľa čl. 4 ods. 2 tejto smernice.

## Článok 2 Vymedzenie pojmov

1. *Manažér kybernetickej bezpečnosti* – štatutárnym orgánom agentúry poverená osoba na výkon riadenia činností kybernetickej bezpečnosti prevádzkovateľa základnej služby (ďalej len „MKB“).
2. *VKB* – Vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.
3. *ZoKB* – Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.

### **Článok 3 Zodpovednosti a právomoci**

1. Za prípravu a aktualizáciu tejto smernice zodpovedá MKB v súčinnosti s poverenou osobou agentúry.
2. Za plnenie povinností podľa tejto smernice sú v primeranom rozsahu zodpovedné osoby podľa čl. 7 vnútorného predpisu č. 2/2024 o bezpečnostnej stratégii kybernetickej bezpečnosti SAAVŠ, najmä štatutárny orgán SAAVŠ, MKB, vedúci kancelárie a ďalší zamestnanci SAAVŠ v rozsahu ich pracovnej náplne, príp. iné osoby, ak to vyplýva z vnútorných predpisov agentúry alebo iných predpisov.

### **Článok 4 Riadenie tretích strán**

1. Riadenie vzťahov s tretími stranami zahŕňa najmä:
  - a) riadenie rizík,
  - b) riadenie dodávateľských zmlúv,
  - c) kontrolnú činnosť (monitorovanie, preskúmavanie, audit),
  - d) riadenie subdodávateľov v rozsahu uzatvorenej zmluvy,
  - e) riadenie incidentov.
2. Vplyv na informačnú a kybernetickú bezpečnosť agentúry majú najmä nasledujúce typy dodávateľov:
  - a) poskytovatelia IT služieb (poskytovatelia cloudových služieb, poskytovatelia bezpečnostných služieb, poskytovatelia hostingových služieb, poskytovatelia outsourcingu),
  - b) dodávatelia a poskytovatelia softvéru,
  - c) dodávatelia hardvéru,
  - d) poskytovatelia telekomunikačných služieb (poskytovatelia internetového pripojenia a komunikačných služieb – dáta aj hlas),
  - e) poskytovatelia tlačových a kopírovacích služieb,
  - f) externí konzultanti a audítori,
  - g) poskytovatelia služieb (upratovacích, bezpečnostných, logistických a pod.).
3. Hodnotenie dodávateľov, ktoré je vyžadované príslušnými predpismi, vykonáva MKB v spolupráci s agentúrou.

### **Článok 5 Riadenie rizík tretích strán**

1. Riadenie rizík tretích strán je podľa § 19 ods. 2 ZoKB a § 9 ods. 1 VKB neoddeliteľnou súčasťou výberu a uzatvárania zmlúv s tretími stranami, ktoré môžu alebo budú mať vplyv na informačnú alebo kybernetickú bezpečnosť agentúry. Priebežné riadenie rizík u existujúcich dodávateľov podľa § 6 ods. 6 bod g) VKB je súčasťou pravidelného (spravidla každoročného) vyhodnotenia procesu riadenia rizík.
2. Tento proces môže byť ďalej vykonaný aj v prípadoch, ktoré predpokladá vnútorný predpis č. 2/2024 o bezpečnostnej stratégii kybernetickej bezpečnosti SAAVŠ – pri

významnej zmene, alebo na žiadosť MKB.

3. Rámcom na vykonanie procesu riadenia rizík vo vzťahu k tretím stranám bude samotný dodávateľ a ním poskytovaná(é) služba(y), ako aj všetky primárne a podporné aktíva agentúry, na ktoré môžu mať alebo majú činnosti tohto dodávateľa určitý vplyv. V prípade dodávateľa cloudových služieb je nevyhnutne a bezodkladne potrebné špecificky vyhodnotiť aspekty zdieľanej zodpovednosti za riadenie bezpečnosti medzi dodávateľom a agentúrou.

## **Článok 6**

### **Dodávateľské zmluvy**

1. Súčasťou zmluvy s dodávateľom musia byť ustanovenia týkajúce sa informačnej a kybernetickej bezpečnosti, za čo sú v primeranom rozsahu zodpovedné osoby podľa čl. 3 ods. 2 tejto smernice.
2. Zmluva s treťou stranou obsahuje aj ustanovenia, ktorých uvedenie v zmluve je povinné podľa zákona č. 513/1991 Zb. Obchodný zákonník, ZoKB, VKB a iných príslušných všeobecne záväzných právnych predpisov.
3. Ustanovenia týkajúce sa informačnej a kybernetickej bezpečnosti môžu byť súčasťou samotnej zmluvy o poskytovaní služieb alebo dodaní tovaru, príp. inej zmluvy uzatváranej s dodávateľom, alebo môžu byť obsiahnuté v samostatnej zmluve.
4. Evidenciu všetkých zmlúv s dodávateľmi vedie oddelenie ekonomiky a prevádzky agentúry. K zmluvám, resp. k ustanoveniam zmlúv relevantným pre kybernetickú a informačnú bezpečnosť má na požiadanie prístup MKB.

## **Článok 7**

### **Kontrola tretích strán**

1. Agentúra môže vykonávať kontrolu dodržiavania bezpečnostných požiadaviek dodávateľom, a to buď priamo, alebo prostredníctvom iných osôb. Dodávateľ a agentúra si za účelom plnenia svojich povinností v oblasti kybernetickej bezpečnosti v súlade s príslušnými právnymi predpismi poskytujú potrebné informácie a súčinnosť.

## **Článok 8**

### **Riadenie subdodávateľov**

1. Od dodávateľov sa vyžaduje, aby propagovali bezpečnostné požiadavky agentúry v celom svojom dodávateľskom reťazci, pokiaľ uzatvárajú subdodávateľské zmluvy týkajúce sa služieb poskytovaných agentúre.

## **Článok 9**

### **Riadenie incidentov**

1. Na riadenie incidentov zistených treťou stranou sa použije štandardný proces

agentúry na riadenie incidentov, formalizovaný v smernici č. 8/2024 o riadení bezpečnostných incidentov SAAVŠ. Tretej strane sa vhodným spôsobom umožní hlásenie incidentov – napr. e-mailom alebo telefonicky v súlade s komunikačnou maticou.

## **Článok 10** **Záverečné ustanovenia**

1. Táto smernica je záväzná pre všetkých zamestnancov agentúry, ktorí sú povinní ju dodržiavať.
2. Za dodržiavanie ustanovení a postupov tejto smernice je zodpovedný vedúci kancelárie agentúry.
3. Výnimku z tejto smernice môže udeliť len predseda výkonnej rady agentúry, resp. ním poverená osoba.
4. Pokiaľ sa niektoré ustanovenia tejto smernice stanú neplatnými alebo neúčinnými, nie je tým dotknutá platnosť a účinnosť celej smernice.
5. Na situácie neupravené touto smernicou sa primerane použijú ustanovenia súvisiacich všeobecne záväzných predpisov a vnútorných predpisov agentúry.
6. Táto smernica nadobúda účinnosť schválením výkonnou radou agentúry dňa 4. septembra 2025.

V Bratislave dňa 4. septembra 2025

**prof. Ing. Robert Redhammer, PhD.**  
predseda výkonnej rady