SLOVENSKÁ AKREDITAČNÁ AGENTÚRA
PRE VYSOKÉ ŠKOLSTVO

VNÚTORNÝ PREDPIS č. 2/2024

BEZPEČNOSTNÁ STRATÉGIA KYBERNETICKEJ BEZPEČNOSTI SLOVENSKEJ AKREDITAČNEJ AGENTÚRY PRE VYSOKÉ ŠKOLSTVO

V Bratislave 29. februára 2024

BEZPEČNOSTNÁ STRATÉGIA KYBERNETICKEJ BEZPEČNOSTI
SLOVENSKEJ AKREDITAČNEJ AGENTÚRY PRE VYSOKÉ ŠKOLSTVO

Výkonná rada Slovenskej akreditačnej agentúry pre vysoké školstvo (ďalej len „výkonná rada“) schválila dňa 29. februára 2024 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 *Bezpečnostnú stratégiu kybernetickej bezpečnosti Slovenskej akreditačnej agentúry pre vysoké školstvo*.

Článok 1
Základné ustanovenia

Bezpečnostná stratégia kybernetickej bezpečnosti (ďalej aj ako „stratégia kybernetickej bezpečnosti“ alebo „stratégia“):

1. tvorí základný strategický dokument pre riadenie informačnej a kybernetickej bezpečnosti v Slovenskej akreditačnej agentúre pre vysoké školstvo (ďalej len „SAAVŠ“ alebo „agentúra“).
2. Tento vnútorný predpis predstavuje záväzok štatutárneho orgánu dodržiavať súlad s platnými zákonmi, nariadeniami a vyhláškami v oblasti kybernetickej bezpečnosti, definuje ciele kybernetickej bezpečnosti, ako aj úlohy a zodpovednosti v tejto oblasti.
3. Dokument zohľadňuje požiadavky zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a súvisiacej legislatívy upravujúcej oblasť informačnej a kybernetickej bezpečnosti.

Článok 2
Zoznam použitých skratiek

Skratka	Vysvetlenie
BCP	Business Continuity Plan; Plán kontinuity činnosti, ktorý definuje postupy pri obnove procesov alebo systémov agentúry v prípade ich prerušenia alebo havárie.
BIA	Business Impact Analysis; Analýza funkčných dopadov; proces identifikovania procesov agentúry, ktoré sú kritické pre potreby poskytovania základných služieb, závislosti týchto procesov a vyhodnotenia dopadu na činnosti agentúry spôsobeného krízovým scenárom. Súčasťou je aj identifikovanie súvisiacich zdrojov potrebných na zabezpečenie prevádzkovej odolnosti, resp. kontinuitu činností počas a po prerušení procesov alebo výpadku systémov. BIA kvantifikuje dopady narušenia na poskytovanie služieb, riziká pre poskytovanie služieb, cieľový čas obnovy (RTO) a cieľový bod obnovy (RPO).

CI	Configuration Item; Konfiguračná položka – akýkoľvek komponent, ktorý je potrebné riadiť za účelom dodávky IT služby. Informácie o každej CI sú zaznamenané v zázname o konfigurácii v systéme konfiguračného manažmentu a udržiavané po celú dobu jej životného cyklu. Konfiguračné položky typicky zahŕňajú IT služby, hardvér, softvér, budovy, ľudí a formálnu dokumentáciu procesov a SLA.
CMMI	Capability Maturity Model Integration; model/metodika na hodnotenie stupňa vyspelosti procesu v agentúre.
DRP	Disaster Recovery Plan; Plán obnovy po havárii, t. j. dokument opisujúci zdroje, činnosti a úlohy zamerané na obnovu informačných systémov, technickej alebo technologickej infraštruktúry v prípade havárie.
GDPR	Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (General Data Protection Regulation).
IB	Informačná bezpečnosť
IKB	Informačná a kybernetická bezpečnosť
IS	Informačný systém
ISO	International Organisation for Standardisation; Medzinárodná štandardizačná organizácia.
IT/IKT	Informačné technológie – technológie na uloženie, odoslanie alebo spracovanie informácií, pričom typicky medzi ne patria počítače, telekomunikácie, aplikácie a ďalší hardvér a softvér.
KB	Kybernetická bezpečnosť
KPI	Key Performance Indicator; ukazovateľ výkonnosti sledovanej oblasti/procesu v čase.
KRI	Key Risk Indicator; ukazovateľ vývinu sledovaného rizika v čase.
MKB	Manažér kybernetickej bezpečnosti
MTD	Maximum Tolerable Downtime; maximálny čas, za ktorý môže organizácia tolerovať nedostupnosť konkrétneho procesu alebo systému.
NBÚ	Národný bezpečnostný úrad
OLA	Dohoda o úrovni prevádzky (Operational Level Agreement) – dohoda medzi poskytovateľom IT služby a inou časťou tej istej organizácie. OLA podporuje dodávku IT služieb zákazníkom od poskytovateľa IT služby. OLA definuje produkty alebo služby, ktoré majú byť poskytované a zodpovednosti oboch strán.
RFC	Požiadavka na zmenu (Request for Change) – formálny návrh na vykonanie zmeny. Obsahuje detaily navrhovanej zmeny a môže byť zaznamenaná v papierovej alebo elektronickej forme.
RPO	Recovery Point Objective; cieľový bod obnovy, t. j. maximálne množstvo dát, ktoré môže byť stratené, kým je proces alebo systém obnovený po jeho prerušení alebo výpadku. Cieľový bod obnovy je vyjadrený ako dĺžka času pred zlyhaním.

RTO	Recovery Time Objective; cieľový čas obnovy, t. j. maximálny prípustný čas na obnovenie procesu alebo systému po jeho prerušení alebo výpadku. RTO musí byť vždy nižšie ako MTD.
SLA	Dohoda o úrovni služby (Service Level Agreement) – dohoda medzi poskytovateľom IT služieb a zákazníkom. SLA popisuje IT službu, dokumentuje cieľovú úroveň služieb a špecifikuje zodpovednosti poskytovateľa IT služby a zákazníka. Jedna SLA môže pokrývať niekoľko služieb IT alebo niekoľko zákazníkov.
Vyhláška o bezpečnostných opatr.	Vyhláška NBÚ č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.
Vyhl. č. 179/2020 Z. z.	Vyhláška ÚPVII č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.
ZS	Základná služba v zmysle zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
ZoITVS	Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov.
ZoKB	Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Článok 3
Úvodné ustanovenia

1. Na zabezpečenie súladu postupov SAAVŠ so ZoKB, ZoITVS, vyhláškou NBÚ č. 362/218 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, vyhláškou Úradu vlády č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení IT verejnej správy, vyhláškou NBÚ č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby), vyhláškou NBÚ č. 165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov, a vyhláškou NBÚ č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora (ďalej len „vyhláška o audite“) a na účely plnenia požiadaviek vyplývajúcich z uvedenej legislatívy sa prijíma táto *Bezpečnostná stratégia kybernetickej bezpečnosti.*

2. Štatutárny orgán SAAVŠ si uvedomuje význam kybernetickej bezpečnosti a jej vplyv na schopnosť agentúry riadne a bezpečne vykonávať jednotlivé činnosti, najmä prevádzkovanie základných služieb zaradených do zoznamu základných služieb vedeného NBÚ. Štatutárny orgán SAAVŠ sa v tomto dokumente zaväzuje k nepretržitej podpore kybernetickej bezpečnosti s cieľom vybudovať a prevádzkovať bezpečný a chránený kybernetický priestor umožňujúci prevádzkovanie základných služieb v požadovanom rozsahu a kvalite.
3. Stratégia kybernetickej bezpečnosti definuje východiská, ciele, záväzky a priority

agentúry v oblasti kybernetickej bezpečnosti v súlade s platnými legislatívnymi požiadavkami a jej poslaním.

4. Stratégia kybernetickej bezpečnosti je východiskovým dokumentom z pohľadu koncepcie kybernetickej bezpečnosti. Na základe stratégie kybernetickej bezpečnosti sa následne vypracúvajú nadväzujúce bezpečnostné smernice, štandardy, postupy, metodické pokyny, prípadne ďalšie dokumenty alebo nástroje slúžiace na zabezpečenie požadovanej úrovne kybernetickej bezpečnosti sietí a informačných systémov SAAVŠ.

Článok 4
Bezpečnostná dokumentácia

Bezpečnostnú dokumentáciu SAAVŠ tvoria tieto dokumenty:

a) stratégia kybernetickej bezpečnosti,
b) bezpečnostná smernica kybernetickej bezpečnosti, súvisiace štandardy, metodiky, pravidlá, postupy a pod.,
c) klasifikácia informácií, informačných systémov a kategorizácia sietí,
d) zadokumentované vymedzenie rozsahu a spôsobu plnenia všetkých bezpečnostných opatrení,
e) dokumentácia súvisiaca s vykonanou analýzou rizík kybernetickej bezpečnosti,
f) záverečná správa o výsledkoch auditu kybernetickej bezpečnosti v zmysle platnej legislatívy.

Článok 5
Bezpečnostné ciele kybernetickej bezpečnosti

1. Cieľom SAAVŠ je zabezpečiť dostupnosť a bezpečnosť poskytovaných základných služieb aj v prípade kybernetického útoku alebo inej udalosti s negatívnym dopadom.
2. Štatutárny orgán SAAVŠ určuje nasledujúce bezpečnostné ciele kybernetickej bezpečnosti:
   a) odolať kybernetickým útokom,
   b) udržať dostupnosť všetkých základných služieb a IS, ktoré ju podporujú,
   c) zaistiť poskytovanie základných služieb v stanovenej kvalite a rozsahu aj pri neštandardných (havarijných) stavoch IS SAAVŠ,
   d) dodržiavať platné právne predpisy a stanovené požiadavky relevantné pre oblasť informačnej a kybernetickej bezpečnosti,
   e) minimalizovať finančné a iné straty súvisiace s narušením prevádzky IS SAAVŠ,
   f) zabezpečiť primeranú úroveň ochrany osobných údajov pri ich spracúvaní,
   g) rozvíjať informačno-komunikačné a bezpečnostné technológie,
   h) zabezpečiť plynulú prevádzku informačných systémov,
   i) identifikovať a minimalizovať riziká ohrozenia aktív,
   j) pravidelne zvyšovať bezpečnostné povedomie zamestnancov agentúry,
   k) chrániť dobré meno agentúry.
3. Plnenie bezpečnostných cieľov je pravidelne vyhodnocované MKB, ktorý na tento účel predkladá štatutárnemu orgánu dokument *Správa o stave kybernetickej bezpečnosti.* Predmetom vyhodnocovania sú najmä:
   a) primeranosť bezpečnostných cieľov,

b) plnenie kritérií dosahovania bezpečnostných cieľov,
c) dodržiavanie postupov využívaných na dosahovanie bezpečnostných cieľov,
d) súlad platnej bezpečnostnej stratégie a bezpečnostných politík s požiadavkami zákona a zmluvnými záväzkami.

4. Kritériami pre vyhodnocovanie dosahovania bezpečnostných cieľov sú najmä:
   a) kľúčové indikátory rizika (KRI),
   b) kľúčové indikátory výkonnosti (KPI),
   c) úroveň vyspelosti bezpečnostných cieľov (napr. podľa rámca CMMI).
5. Bezpečnostné ciele sú prehodnocované pravidelne 1x ročne na úrovni štatutárneho orgánu.
6. Bezpečnostné ciele sú vyhodnocované nasledujúcim spôsobom:

	Cieľ	Spôsob	Kritériá vyhodnotenia	Periodicita
1.	Odolať kybernetickým útokom	Počet úspešných kybernetických útokov, v dôsledku ktorých došlo ku kompromitácii dôvernosti, integrity	Žiadny úspešný útok v priebehu jedného kalendárneho roka	štvrťročne
2.	Udržať dostupnosť všetkých základných služieb a IS, ktoré ju podporujú	Počet hodín nedostupnosti základnej služby mimo platných SLA	Žiadne nežiaduce prerušenie prevádzky základnej služby v priebehu jedného kalendárneho roka v rámci platných SLA	štvrťročne
3.	Zaistiť poskytovanie ZS v stanovenej kvalite a rozsahu aj pri neštandardných (havarijných) stavoch IS SAAVŠ	Počet hodín nedostupnosti základnej služby alebo jej zníženej kvality mimo platných SLA	Zachovanie požadovanej úrovne služby a dodržanie postupov kontinuity procesov a činností – BCP a DRP plánov v rámci platných SLA	štvrťročne
4.	Dodržiavať právne predpisy a stanovené požiadavky relevantné pre oblasť IKB	Počet udelených pokút, počet nálezov pri audite IKB	Žiadna pokuta udelená kontrolným orgánom	štvrťročne
5.	Minimalizovať finančné a iné straty súvisiace s narušením prevádzky IS SAAVŠ	Výška strát a nákladov súvisiacich s narušením IS SAAVŠ	Žiadne straty a náklady súvisiace s narušením a obnovením prevádzky IS SAAVŠ	štvrťročne

6.	Zabezpečiť primeranú úroveň ochrany údajov pri ich spracúvaní	Počet porušení ochrany osobných údajov	Žiadne porušenia ochrany osobných údajov	štvrťročne
7.	Rozvíjať informačno-komunikačné a bezpečnostné technológie	Plán rozvoja IKT a bezpečnostných technológií	Plnenie plánu rozvoja IKT a bezpečnostných technológií	štvrťročne
8.	Zabezpečiť plynulú prevádzku informačných systémov	Počet prerušení IS SAAVŠ mimo platných SLA	Žiadne prerušenia IS SAAVŠ, resp. adekvátna reakcia použitím procesov riadenia kontinuity v rámci platných SLA	štvrťročne
9.	Identifikácia a minimalizácia rizík ohrozenia aktív IS	Pravidelné vykonávanie analýzy rizík	Počet identifikovaných a odstránených zostatkových rizík	štvrťročne
10.	Pravidelne zvyšovať bezpečnostné povedomie	Plán zvyšovania bezpečnostného povedomia zamestnancov	Počet vykonaných školení/ vyhodnotenie jednotlivých školení	štvrťročne
11.	Chrániť dobré meno agentúry	Počet negatívnych správ v médiách týkajúcich sa kyb. bezpečnosti	Žiadne negatívne PR správy v súvislosti s kybernetickou bezpečnosťou	štvrťročne

Článok 6
Úlohy štatutárneho orgánu pri zabezpečovaní kybernetickej bezpečnosti

Štatutárny orgán SAAVŠ pri zabezpečovaní kybernetickej bezpečnosti plní nasledovné úlohy:

a) predkladá na schválenie Stratégiu kybernetickej bezpečnosti,
b) schvaľuje príslušné nadväzné súčasti bezpečnostnej dokumentácie (článok 4),
c) na základe záväzku podpory kybernetickej bezpečnosti zabezpečuje primerané personálne, materiálne, technické a finančné zdroje potrebné na dosiahnutie bezpečnostných cieľov kybernetickej bezpečnosti,
d) umožňuje MKB priamo mu predkladať návrhy a oznamovať informácie v oblasti kybernetickej bezpečnosti, najmä informácie o stave systému riadenia kybernetickej bezpečnosti,
e) bez zbytočného odkladu informuje MKB o všetkých skutočnostiach, ktoré by mohli mať vplyv na identifikačné kritériá už registrovanej prevádzkovanej základnej služby alebo ktoré by mohli mať vplyv na to, že SAAVŠ bude vykonávať takú činnosť, pri ktorej by došlo k prekročeniu identifikačných kritérií základnej služby (najmä informácie o zmene v predmete činnosti agentúry a pod.),
f) poskytne MKB súčinnosť v takom rozsahu, ktorá je potrebná na to, aby bolo možné vyhodnotiť, či SAAVŠ vykonáva činnosť, ktorá je považovaná za základnú službu v

zmysle príslušných všeobecne záväzných právnych predpisov v oblasti kybernetickej bezpečnosti.

Článok 7
Práva a povinnosti osôb v oblasti kybernetickej bezpečnosti

1. Práva a povinnosti osôb v oblasti kybernetickej bezpečnosti zahrňujú riadiacu, výkonnú a kontrolnú zložku v nasledovnom členení.
2. Štatutárny orgán SAAVŠ predstavuje riadiacu a rozhodovaciu zložku najvyššej úrovne pri zabezpečovaní kybernetickej bezpečnosti. Prijíma záväzok týkajúci sa schvaľovania systému riadenia kybernetickej bezpečnosti, záväzok o podpore kybernetickej bezpečnosti zabezpečovaním potrebných zdrojov a schvaľovaním príslušných dokumentov.
3. MKB predstavuje výkonnú zložku v oblasti kybernetickej bezpečnosti, zabezpečuje implementáciu bezpečnostných opatrení spolu so zamestnancami zabezpečujúcimi informačné technológie SAAVŠ a zodpovedá za predkladanie návrhov štatutárnemu orgánu SAAVŠ.
4. Externý audítor spolu s vedúcim kancelárie SAAVŠ predstavujú kontrolnú zložku v oblasti kybernetickej bezpečnosti. Kontrolná zložka je nezlučiteľná s ostatnými zložkami a zabezpečuje kontrolu pravidiel a povinností v oblasti kybernetickej bezpečnosti.
5. Zamestnanci SAAVŠ predstavujú výkonnú zložku a sú povinní dodržiavať pravidlá, zásady a bezpečnostné opatrenia v oblasti kybernetickej bezpečnosti vyplývajúce z príslušných interných predpisov agentúry.
6. Rozsah činností, kompetencií a úloh jednotlivých osôb bude upravený v organizačnom poriadku SAAVŠ.

Článok 8
Základný rámec riadenia aktív

1. Riadenie aktív je súbor činností zabezpečujúcich správu aktív počas celého životného cyklu – od plánovania, obstarania, prevádzky, údržby, obnovy až po likvidáciu. Riadenie aktív a rizík v oblasti kybernetickej bezpečnosti je proces spojený s finančnými, zmluvnými a inventarizačnými funkciami na podporu riadenia životného cyklu informačných technológií a konfiguračných položiek.
2. Za aktívum sa považuje všetko, čo má pre SAAVŠ hodnotu (napr. hardvérové komponenty, softvér, informácie, služby, ľudské zdroje, dobré meno agentúry a pod.).
3. Základný rámec riadenia aktív SAAVŠ pozostáva najmä z identifikácie a evidencie:
   a) všetkých aktív, od ktorých závisí činnosť sietí a informačných systémov a poskytovanie základných služieb,
   b) všetkých podporných služieb, prostredníctvom ktorých sa zabezpečuje kontinuita základnej služby a jej poskytovania,
   c) všetkých zodpovedných osôb za identifikáciu a evidenciu aktív,
   d) všetkých vlastníkov aktív.
4. Všetky aktíva súvisiace so zariadeniami na spracovanie informácií a informačnými prostriedkami sú v prostredí SAAVŠ identifikované a inventár týchto aktív je

centrálne evidovaný, zaznamenaný a riadený.
5. Rámec riadenia aktív je bližšie špecifikovaný vo vnútorných predpisoch SAAVŠ.

Článok 9
Základný rámec riadenia rizík

1. Riadenie rizík je implementovaný a neustále sa opakujúci proces riadenia informačných a kybernetických rizík počas celého ich životného cyklu.
2. Základný rámec riadenia rizík vychádza z noriem:
   a) STN ISO 31000 Manažérstvo rizika – Návod,
   b) STN EN IEC 31010 Manažérstvo rizika, Techniky posudzovania rizík,
   c) STN ISO/IEC 27005 Informačné technológie, Bezpečnostné metódy, Riadenie rizík informačnej bezpečnosti.
3. Zodpovednosť za riadenie rizík informačnej bezpečnosti SAAVŠ nesie štatutárny orgán, ktorý touto úlohou poveruje MKB. Rámec riadenia informačných a kybernetických rizík je bližšie špecifikovaný v internom predpise SAAVŠ upravujúcom riadenie bezpečnostných rizík.
4. Základný rámec riadenia rizík SAAVŠ v súvislosti s aktívami, od ktorých závisí činnosť sietí a informačných systémov, pozostáva najmä z:
   a) pravidelného a kontinuálneho monitoringu siete,
   b) identifikácie zraniteľností,
   c) identifikácie hrozieb,
   d) identifikácie a analýzy rizík s ohľadom na aktívum,
   e) určenia vlastníka rizika,
   f) implementácie organizačných a technických bezpečnostných opatrení v závislosti od identifikovaných rizík vrátane informácie, ktoré bezpečnostné opatrenia sú implementované a ktoré bezpečnostné opatrenia nie sú implementované spolu s odôvodnením,
   g) analýzy funkčného dopadu,
   h) pravidelného preskúmavania identifikovaných rizík a v závislosti od toho aktualizácie prijatých bezpečnostných opatrení.
5. Identifikácia hrozieb je založená na identifikácii aktív a ich vlastníkov a identifikácii zraniteľností potenciálne pôsobiacich na tieto aktíva.
6. Identifikácia rizika sa vykonáva na základe princípu najhoršieho scenára, ktorý môže nastať aj pri nízkej pravdepodobnosti.
7. Preskúmavanie rizík sa vykonáva pravidelne 1x ročne a pri každej významnej zmene prostredia.
8. Pravidlá a zásady riadenia informačných a kybernetických rizík sú bližšie špecifikované v internom predpise SAAVŠ upravujúcom riadenie bezpečnostných rizík.

Článok 10
Rozsah a periodicita overovania stavu kybernetickej bezpečnosti

1. Overovanie stavu kybernetickej bezpečnosti, účinnosti prijatých bezpečnostných opatrení a plnenia požiadaviek stanovených platnou legislatívou sa overuje prostredníctvom auditu kybernetickej bezpečnosti v súlade s vyhláškou o audite,

vrátane zhodnotenia súladu Stratégie kybernetickej bezpečnosti a bezpečnostnej dokumentácie s požiadavkami platnej legislatívy, interných predpisov SAAVŠ a jej zmluvnými záväzkami.
2. Audit kybernetickej bezpečnosti sa vykonáva po každej zmene majúcej významný vplyv na realizované bezpečnostné opatrenia a v časovom intervale určenom platnou legislatívou.
3. Záverečná správa o výsledkoch auditu kybernetickej bezpečnosti je predkladaná NBÚ spolu s opatreniami na nápravu a lehotami na ich odstránenie.
4. Audit kybernetickej bezpečnosti vykonáva certifikovaný audítor kybernetickej bezpečnosti v súlade s postupom a metodikou v zmysle platnej legislatívy. Lehoty na vykonanie auditu kybernetickej bezpečnosti, ako aj ostatné povinnosti a zodpovednosti SAAVŠ súvisiace s auditom kybernetickej bezpečnosti sú podrobne popísané v príslušnom internom predpise SAAVŠ.
5. Priebežné overovanie stavu kybernetickej bezpečnosti a miery napĺňania legislatívnych požiadaviek je vykonávané interným alebo externým MKB alebo audítorom kybernetickej bezpečnosti.

Článok 11
Postupy a zodpovednosti pri revízii bezpečnostnej dokumentácie

1. Bezpečnostná dokumentácia pre oblasť kybernetickej bezpečnosti ako základ stanovenia a dodržiavania bezpečnostných opatrení sa v primeranej miere aktualizuje a pravidelne reviduje aspoň 1x ročne alebo na základe všetkých zmien, ktoré majú vplyv na jej obsah.
2. Za revíziu bezpečnostnej dokumentácie zodpovedá MKB.

Článok 12
Záverečné ustanovenia

1. Stratégia kybernetickej bezpečnosti je záväzná pre všetkých zamestnancov agentúry, ktorí sú povinní sa s ňou preukázateľne oboznámiť.
2. Táto Stratégia kybernetickej bezpečnosti nadobúda platnosť a účinnosť dňom jej schválenia výkonnou radou dňa 29. februára 2024.

V Bratislave 29. februára 2024

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