

## BEZPEČNOSTNÁ STRATÉGIA KYBERNETICKEJ BEZPEČNOSTI

### A: Štruktúra bezpečnostnej stratégie kybernetickej bezpečnosti

Bezpečnostná stratégia kybernetickej bezpečnosti obsahuje najmenej určenie

1. bezpečnostných cieľov z hľadiska kybernetickej bezpečnosti,
2. spôsobu vyhodnocovania bezpečnostných cieľov, kritérií vyhodnocovania dosahovania bezpečnostných cieľov, spôsobov priebežného hodnotenia ich primeranosti a spôsobov kontroly postupov využívaných na dosahovanie bezpečnostných cieľov,
3. úlohy štatutárneho orgánu prevádzkovateľa základnej služby pri zabezpečovaní kybernetickej bezpečnosti a vyhlásenie o záväzku o podpore kybernetickej bezpečnosti,
4. všeobecných a špecifických zodpovedností a povinností v oblasti kybernetickej bezpečnosti a určenie príslušných bezpečnostných rolí potrebných na riadenie kybernetickej bezpečnosti vrátane určenia rozsahov činností, kompetencií a úloh; rozdelenie rolí na riadiacu zložku, výkonnú zložku a kontrolnú zložku, pričom riadiaca zložka je priamo riadená prevádzkovateľom základnej služby a kontrolná zložka je nezlučiteľná so všetkými ostatnými zložkami,
5. základného rámca na riadenie aktív podľa § 6, od ktorých závisí činnosť sietí a informačných systémov,
6. základného rámca riadenia rizík podľa § 6 v súvislosti s aktívami, od ktorých závisí činnosť sietí a informačných systémov a určenie bezpečnostných opatrení podľa oblastí v zmysle § 20 ods. 3 zákona v závislosti od identifikovaných rizík,
7. rozsahu a periodicity overovania stavu kybernetickej bezpečnosti prostredníctvom auditu kybernetickej bezpečnosti vrátane zhodnotenia súladu bezpečnostnej stratégie a bezpečnostných politík s požiadavkami zákona, iného všeobecne záväzného právneho predpisu, vnútorných predpisov a zmluvnými záväzkami,
8. postupu a zodpovedností pri revízii bezpečnostnej dokumentácie schvaľovanej prevádzkovateľom základnej služby vrátane periodicity pravidelných revízií a jej aktualizácií po každej zmene majúcej na ňu vplyv, ako aj z dôvodov mimoriadnych revízií.

## B: Štruktúra bezpečnostnej politiky kybernetickej bezpečnosti

Bezpečnostné politiky	Súvisiace bezpečnostné štandardy
<b>1. Organizácia bezpečnosti</b>	<ul style="list-style-type: none"><li>– Riadenie bezpečnostnej architektúry</li><li>– Systém riadenia kybernetickej bezpečnosti</li><li>– Riadenie identít a prístupových práv</li><li>– Riadenie privilegovaných prístupov</li><li>– Bezpečnostný monitoring a správa bezpečnostných záznamov</li></ul>
<b>2. Riadenie bezpečnostných rizík</b>	<ul style="list-style-type: none"><li>– Testovanie a bezpečnostná certifikácia systémov</li><li>– Metodika posudzovania vplyvu na ochranu osobných údajov</li><li>– Metodika posudzovania rizík</li><li>– Fyzická bezpečnosť a bezpečnosť prostredia</li><li>– Riešenie bezpečnostných incidentov</li></ul>
<b>3. Riadenie informačných aktív</b>	<ul style="list-style-type: none"><li>– Klasifikácia informácií a kategorizácia sietí</li><li>– Registratúrny poriadok a registratúrny plán</li></ul>
<b>4. Pravidlá správania a dobrej praxe</b>	<ul style="list-style-type: none"><li>– Práca na diaľku a používanie mobilných zariadení</li><li>– Riadenie personálnej bezpečnosti</li><li>– Pravidlá komunikácie</li></ul>
<b>5. Riadenie dodávateľských vzťahov</b>	<ul style="list-style-type: none"><li>– Riadenie dodávateľských služieb</li><li>– Akvizícia informačných systémov</li></ul>
<b>6. Riadenie vývoja a údržby v oblasti informačno-komunikačných technológií</b>	<ul style="list-style-type: none"><li>– Vývoj a testovanie informačných systémov</li><li>– Postupy údržby informačných systémov</li><li>– Riadenie technických zraniteľností a manažment záplat</li></ul>
<b>7. Riadenie a prevádzka informačno-komunikačných technológií</b>	<ul style="list-style-type: none"><li>– Pravidlá prepájania systémov a prenosu elektronických informácií</li><li>– Riadenie bezpečnosti sietí</li><li>– Riadenie zmien infraštruktúry</li><li>– Riadenie kapacity systémov a služieb</li><li>– Riadenie kryptografických opatrení</li></ul>
<b>8. Riadenie súladu</b>	<ul style="list-style-type: none"><li>– Audit kybernetickej bezpečnosti</li><li>– Spracúvanie osobných údajov a klasifikovaných informácií</li><li>– Poskytovanie súčinnosti tretím stranám</li></ul>
<b>9. Riadenie kontinuity procesov a činností</b>	<ul style="list-style-type: none"><li>– Plány kontinuity prevádzkových činností</li><li>– Plány havarijnej obnovy prevádzky</li><li>– Metodika zálohovania a obnovy informácií</li></ul>