„Návrh“

**VYHLÁŠKA**

**Úradu pre reguláciu elektronických komunikácií a poštových služieb**

z … /2024

**o podrobnostiach uznávania školiaceho strediska**

Úrad pre reguláciu elektronických komunikácií a poštových služieb (ďalej len „úrad“) podľa § 52a zákona č. 452/2021 Z. z. o elektronických komunikáciách v znení zákona č. .../2024 Z. z. (ďalej len „zákon“) ustanovuje:

**§ 1**

**Technické vybavenie školiaceho strediska**

Minimálnym technickým vybavením školiaceho strediska je toto vybavenie:

1. dve rádiostanice VHF DSC triedy D, prepojené „back to back“,
2. prepojovací box pre prepojenie rádiostaníc s útlmovým článkom (umelá anténa),
3. aspoň jedna rádiostanica VHF DSC triedy D so zabudovaným GPS prijímačom, alebo externý GPS prijímač prepojený aspoň s jednou rádiostanicou VHF DSC D,
4. napájací zdroj vhodný pre napájanie rádiostaníc vrátane príslušnej elektrickej inštalácie a platnej elektrickej revízie,
5. jedna prenosná rádiostanica GMDSS VHF,
6. príslušenstvo pre dobíjanie interných akumulátorových batérií pre demonštráciu nabíjania pri školení,
7. jeden prijímač NAVTEX,
8. jedna výcviková maketa EPIRB bóje 406 MHz,
9. jedna výcviková maketa SART 9 GHz.

**§ 2**

**Plán praktického výcviku**

Náležitosti plánu praktického výcviku sú uvedené v prílohe.

**§ 3**

**Účinnosť**

Táto vyhláška nadobúda účinnosť ……. 2024.

**Príloha č. 1**

**k vyhláške č. .../2024 Z. z.**

**Náležitosti plánu praktického výcviku**

1. Identifikačné údaje školiaceho strediska podľa § 52a odsek 3 písm. a) zákona.

2. Vymedzenie odborných znalostí a zručností, ktoré majú uchádzači získať absolvovaním praktického výcviku. 3. Vymedzenie počtu hodín určených získavaniu príslušných znalostí a zručností praktického výcviku, spolu najmenej desať hodín.

4. Určenie maximálneho počtu účastníkov praktického výcviku, pričom maximálny počet účastníkov jedného praktického výcviku je dvojnásobok počtu rádiostaníc podľa § 1 písm. a).

5. Popis materiálneho zabezpečenia a technického vybavenia, vrátane literatúry, ktorá bude k dispozícii.

„Návrh“

**VYHLÁŠKA**

**Národného bezpečnostného úradu**

z .............,

**ktorou sa určujú podrobnosti o hláseniach**

Národný bezpečnostný úrad (ďalej len „úrad“) podľa [§ 32 ods. 1 písm. i) zákona č. 69/2018](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/69/#paragraf-32.odsek-1.pismeno-e) Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení zákona č. …/2024 (ďalej len „zákon“) ustanovuje:

**§ 1**

(1) Hlásenie podľa § 24 zákona obsahuje, v rozsahu potrebnom na riadnu identifikáciu, najmä informácie

a) o tom, kto hlási závažný kybernetický bezpečnostný incident, a to

1. identifikačné údaje a

2. kontaktné údaje,

b) o závažnom kybernetickom bezpečnostnom incidente, a to

1. časové údaje priebehu kybernetického bezpečnostného incidentu,

2. detailný opis priebehu kybernetického bezpečnostného incidentu a

3. rozsah vzniknutých škôd z dôvodu kybernetického bezpečnostného incidentu,

c) o službe zasiahnutej závažným kybernetickým bezpečnostným incidentom, a to

1. konkrétny popis všetkých zasiahnutých aktív a

2. vplyv kybernetického bezpečnostného incidentu na poskytovanú službu,

d) o riešení závažného kybernetického bezpečnostného incidentu, a to

1. stav riešenia kybernetického bezpečnostného incidentu,

2. vykonané nápravné opatrenia a

3. popis následkov kybernetického bezpečnostného incidentu.

(2) Vzor hlásenia kybernetických bezpečnostných incidentov zverejňuje úrad prostredníctvom jednotného informačného systému kybernetickej bezpečnosti a na svojom webovom sídle.

**§ 2**

Touto vyhláškou sa preberajú právne záväzné akty Európskej únie uvedené v prílohe.

**§ 3**

Táto vyhláška nadobúda účinnosť …

Roman Konečný, v. r.

**Príloha**

**k vyhláške č. … Z. z.**

**Zoznam preberaných právne záväzných aktov Európskej únie**

Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2) (Ú.v. EÚ L 333, 27.12.2022) v platnom znení.“.

„Návrh“

**V Y H L Á Š K A**

**Národného bezpečnostného úradu**

z ... ,

**ktorou sa mení a dopĺňa vyhláška Národného bezpečnostného úradu č. 493/2022 Z. z.   
o audite kybernetickej bezpečnosti**

Národný bezpečnostný úrad podľa [§ 32 ods. 1](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/69/20210801#paragraf-32.odsek-1.pismeno-d) písm. d) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení zákona č. 287/2021 Z. z. a zákona č. .../2024 Z. z. ustanovuje:

**Čl. I**

Vyhláška Národného bezpečnostného úradu č. 493/2022 Z. z. o audite kybernetickej bezpečnosti sa mení a dopĺňa takto:

1. V § 1 ods. 1 prvej vete sa za slová „Auditom kybernetickej bezpečnosti“ vkladajú slová „alebo samohodnotením“ a v druhej vete sa za slovo „Auditom“ vkladajú slová „alebo samohodnotením“.
2. V § 1 ods. 2 sa na konci pripája táto veta:

„Samohodnotenie vykonáva manažér kybernetickej bezpečnosti podľa § 29 ods. 8 zákona.“.

1. V § 1 ods. 3 sa na konci pripája táto veta:

„Na vykonanie samohodnotenia manažér kybernetickej bezpečnosti spĺňa podmienky znalostného štandardu podľa osobitného predpisu.2a)“.

Poznámka pod čiarou k odkazu 2a znie:

„2a) Vyhláška Národného bezpečnostného úradu č. 492/2022 Z. z., ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti.“.

1. V § 1 ods. 4 sa na konci pripája táto veta:

„Manažér kybernetickej bezpečnosti zodpovedá za pravdivé a úplné vyplnenie formulára samohodnotenia podľa prílohy č. 4 a zabezpečuje doručenie výsledku samohodnotenia úradu bezodkladne po jeho vykonaní.“.

1. V § 1 ods. 5 sa na konci pripája táto veta:

„Manažér kybernetickej bezpečnosti vypĺňa formulár samohodnotenia na základe aktuálneho stavu v prostredí prevádzkovateľa základnej služby pravdivo a tak, aby uvedené odpovede bolo možné v prípade potreby preveriť.“.

1. V § 1 ods. 6 sa za slovo „auditu“ vkladajú slová „alebo samohodnotenia“.
2. § 1 sa dopĺňa odsekom 8, ktorý znie:

„(8) Prevádzkovateľ základnej služby, ktorý nie je prevádzkovateľom kritickej základnej služby, vykonáva samohodnotenie prostredníctvom jednotného informačného systému kybernetickej bezpečnosti vyplnením formulára podľa prílohy č. 4.“.

1. § 2 sa dopĺňa odsekom 5, ktorý znie:

„(5) Výsledok samohodnotenia vyhodnocuje úrad.“.

1. V Prílohe č. 1 ôsmom bode sa slová „§ 20 ods. 5“ nahrádzajú slovami „§ 20 ods. 6“.
2. V Prílohe č. 2 písmeno B vrátane nadpisu znie:

„B URČENIE ČASOVÉHO INTERVALU AUDITU A SAMOHODNOTENIA

1. Audit sa vykonáva
2. každé dva roky, pričom audit sa musí začať do dvoch rokov od vydania záverečnej správy o výsledkoch auditu,
3. pri každej významnej zmene, najneskôr do dvoch mesiacov, odkedy má zmena významný vplyv na realizované bezpečnostné opatrenia,
4. každých šesť rokov u prevádzkovateľa základnej služby, ktorý nie je prevádzkovateľom kritickej základnej služby.
5. Samohodnotenie sa vykonáva každé dva roky, pričom v čase vykonania auditu podľa písmena c) sa samohodnotenie.
6. Významným vplyvom sa rozumie najmä
7. vplyv na prijatú klasifikáciu informácií a kategorizáciu sietí a informačných systémov,
8. zmena alebo výmena informačného systému a prevádzkových parametrov základnej služby,
9. zavedenie novej siete, nového informačného systému, od ktorých je závislá základná služba,
10. zavedenie novej technológie, od ktorej je závislá základná služba, alebo
11. zmena systémovej architektúry alebo sieťovej topológie.“.
12. Príloha č. 4 vrátane nadpisu znie:

SAMOSTATNÁ PRÍLOHA

**Čl. II**

Táto vyhláška nadobúda účinnosť ...

Roman Konečný, v. r.

„Návrh“

**VYHLÁŠKA**

**Národného bezpečnostného úradu**

z .............

**o základných zručnostiach pri zabezpečovaní kybernetickej bezpečnosti**

**a budovaní bezpečnostného povedomia**

Národný bezpečnostný úrad podľa § 32 ods. 1 písm. h) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení zákona č. .../2024 Z. z. ustanovuje:

**§ 1**

**Predmet úpravy**

Táto vyhláška upravuje základné zručnosti pri zabezpečovaní kybernetickej bezpečnosti a budovanie bezpečnostného povedomia. Základné zručnosti predstavujú minimálny štandard postupov a opatrení, ktorých cieľom je zvýšenie úrovne kybernetickej bezpečnosti.

**§ 2**

**Základné zručnosti**

(1) Základné zručnosti predstavujú politiky

a) postupov a aktualizácie softvéru a hardvéru,

b) zmeny hesiel,

c) riadenia nových inštalácií,

d) obmedzenia prístupových účtov na úrovni správcu a zálohovania údajov,

e) budovania bezpečnostného povedomia.

(2) Politiky podľa odseku 1 písm. a) až d) musia zodpovedať aktuálnemu stavu.

**§ 3**

**Politika postupov a aktualizácie hardvéru a softvéru**

Politika postupov a aktualizácie softvéru a hardvéru podľa § 2 ods. 1 písm. a) obsahuje najmä

1. používanie kvalitných komponentov a ich údržba,
2. pravidlá používania aplikácií z overených zdrojov,
3. sledovanie a kontrola prístupu,
4. pravidlá ochrany pred neoprávneným prístupom, výpadkom energií,
5. používanie šifrovacích zariadení,
6. používanie a inštaláciu **antivírusového** a antimalwarového softvéru,
7. nastavenia funkcií pre automatické aktualizácie softvéru,
8. ochranu bezpečnostného rozhrania (firewall).

**§ 4**

**Politika zmeny hesiel**

Politika zmeny hesiel podľa § 2 ods. 1 písm. b) obsahuje najmä definovanie zásad zmeny hesiel v zrozumiteľnej forme, dodržiavanie politiky hesiel na všetkých úrovniach, ochranu ukladaných používateľských hesiel a zásady ich zmien.

**§ 5**

**Politika riadenia nových inštalácií**

Politika riadenia nových inštalácií podľa § 2 ods. 1 písm. c) zahŕňa najmä pravidlá inštalácie ovládačov pre komponenty a určenie postupov pre prípad update softvéru.

**§ 6**

**Politika obmedzenia prístupových účtov a zálohovanie údajov**

Politika obmedzenia prístupových účtov na úrovni správcu a zálohovania údajov podľa § 2 ods. 1 písm. d) obsahuje najmä

1. zavedenie princípu minimálnych právomocí,
2. vytvorenie oddelených prístupových účtov,
3. určenie postupov zálohovania údajov v prípade poškodenia alebo zlyhania hardvéru,
4. zásady ochrany údajov pred ich stratou alebo poškodením.

**§ 7**

**Bezpečnostné povedomie**

(1) Budovanie bezpečnostného povedomia podľa § 2 ods. 1 písm. e) zahŕňa najmä vzdelávanie o obsahu politík podľa § 2 ods. 1 písm. a) až d), o základoch kybernetickej bezpečnosti a vykonávanie simulovaného testovania, jeho analyzovanie a vyhodnocovanie.

(2) Vzdelávanie a vykonávanie simulovaného testovania podľa odseku 1 sa vykonáva pravidelne, minimálne jedenkrát ročne.

**§ 8**

**Účinnosť**

Táto vyhláška nadobúda účinnosť .............. .

Roman Konečný, v.r.