NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Návod na vyplnenie formuláru Samohodnotenie v zmysle zákona o kybernetickej bezpečnosti

---

Obsah dokumentu:

27.9.2021

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Úvod

Vážený prevádzkovateľ základnej služby (PZS),

tento návod je určený k formuláru na samohodnotenie v zmysle zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 69/2018 Z. z.“).

Formulár na samohodnotenie je určený pre tých poskytovateľov základných služieb, ktorí:

1. majú v období od 1. augusta 2021 do 31. decembra 2023 povinnosť auditu podľa zákona č. 69/2018 Z. z.,
2. majú len informačné systémy kategórie I. a II. podľa vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „vyhláška č. 362/2018 Z. z.“) a
3. majú určeného manažéra kybernetickej bezpečnosti.

Formulár je určený k vyplneniu za PZS určeným manažérom kybernetickej bezpečnosti na základe aktuálneho stavu v prostredí PZS pravdivo a tak aby uvedené odpovede bolo možné v prípade potreby preveriť. K jednotlivým otázkam je odporúčané pripojiť referenciu na dokumenty podporujúce vyplnené tvrdenia.

K vyplnenému formuláru je potrebné priložiť **plán implementácie opatrení kybernetickej bezpečnosti** na nasledujúce obdobie schválené štatutárom.

Vyplnený formulár s plánom implementácie opatrení je potrebné elektronicky podpísať kvalifikovaným elektronickým podpisom štatutára a zaslať e-mailom na *podatelna@nbu.gov.sk*, prípadne zaslať do elektronickej schránky Národného bezpečnostného úradu (NBÚ) prostredníctvom ÚPVS (slovensko.sk).

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Technický návod na elektronické vyplnenie formuláru

Pre elektronické vypĺňanie formulárov odporúčame dokument stiahnuť na pevný disk a použiť aktuálnu verziu jednej za nasledovných aplikácií:

- MS Windows: Adobe Reader (verzia 11 a novšia)
- PDF-XChange Editor
- Foxit Reader
- Adobe Acrobat Reader pre Android

Pri vypĺňaní formulára vyplňte odpovede vo formáte závislom od typu otázky (dátumy sú vo formáte DD.MM.YYYY). Po vyplnení formuláru priložte elektronický podpis a následne dokument uložte. Pred odoslaním dokument znovu otvorte, aby ste skontrolovali, že sa vyplnené odpovede uložili.

Vyplnený fomulár následne zašlite e-mailom na podatelna@nbu.gov.sk, prípadne do elektronickej schránky NBÚ prostredníctvom ÚPVS (slovensko.sk).

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Metodický návod na elektronické vyplnenie formuláru

Väčšina otázok vo formulári požaduje jednoduchú formu odpovede, buď v podobe textu, dátumu alebo odpoveď áno/nie.

Na zodpovedanie otázok ohľadom implementácie procesov použite nasledovnú metódu:

F.1 Máte identifikované všetky informačné aktíva, ktoré podporujú niektorú z identifikovaných ZS?

◯ Áno ◯ Nie ◯ Čiastočne

Príslušný dokument (voliteľné):

Na posúdenie odpovede na otázku ohľadom implementácie procesu vrámci vášho PZS posúďte nasledovné tvrdenia:

- Činnosti daného procesu sú interne definované
- Činnosti daného procesu sú zdokumentované
- Činnosti daného majú určené rozdelenie povinností a príslušných rolí
- Činnosti daného procesu sú vykonávané pravidelne

V prípade, že sú všetky tvrdenia pravdivé, zvoľte odpoveď **Áno.**
V prípade, že aspoň jedno tvrdenie je pravdivé, zvoľte odpoveď **Čiastočne.**
V prípade, že nie je žiadne tvrdenie pravdivé, zvoľte odpoveď **Nie.**

Na potvrdenie Vášho tvrdenia odporúčame pridať názov príslušného dokumentu, v ktorom je daný proces zdokumentovaný, resp. je výsledkom danej činnosti.

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Vysvetlenie otázok s uvedenými príkladmi odpovedí

V nasledujúcej sekcii nájdete zoznam všetkých otázok s ich vysvetleniami, príslušnými zákonmi, a príkladnými odpoveďami.

Časť A: Identifikácia PZS

Identifikácia prevádzkovateľa základných služieb.
PZS = prevádzkovateľ základných služieb
JISKB = Jednotný informačný systém kybernetickej bezpečnosti

Otázka A.1 Názov PZS
Vysvetlenie: Názov PZS, pod ktorým je uvedený v JISKB
Príklad odpovede: Datastore, s.r.o.

A.2 Sídlo PZS
Aktuálna adresa sídla PZS
Kybernetická 362, 853 07 Bratislava

A.3 IČO PZS
Identifikačné číslo organizácie prevádzkovateľa základných služieb
35872844

A.4 Meno a priezvisko štatutára
Meno aktuálneho štatutára prevádzkovateľa základných služieb
Ing. Peter Chudý

A.5 Dátum zaradenia PZS do registra PZS
Dátum zaradenia prevádzkovateľa základných služieb do registra podľa oznámenia NBÚ.
22.10.2019

Časť B: Základná služba

Zaregistrované základné služby. Túto sekciu treba vyplniť pre každú zaregistrovanú službu zvlášť.
ZoKB = Zákon o kybernetickej bezpečnosti (§17 zákona č. 69/2018 Z. z.)

B.1 Názov základnej služby
Názov základnej služby podľa oznámenia NBÚ
Laboratórne služby

B.2 Sektor
Podľa oznámenia NBÚ podľa ZoKB, príloha č.1.
Zdravotníctvo

B.3 Podsektor
Podľa oznámenia NBÚ podľa ZoKB, príloha č.1.
Zdravotnícke zariadenia

B.4 Dátum zápisu základnej služby do zoznamu základných služieb
Dátum zápisu základnej služby do registra podľa oznámenia NBÚ
22.10.2019

Časť C: Manažér KB

Identifikácia určeného manažéra kybernetickej bezpečnosti a vyjadrenie sa k popisu jeho právomoci, povinnosti a zodpovednosti, ktoré sú súčasťou jeho pracovnej náplne alebo obdobného opisu jeho pracovných činností.
(§20 ods. 3 písm. a) zákona č. 69/2018 Z. z. a § 5 vyhlášky č. 362/2018 Z. z.)
KB = Kybernetická bezpečnosť

C.1 Meno a priezvisko manažéra KB
Meno aktuálneho určeného manažéra KB
Ing. Ondrej Rozumný

C.2 Dátum nástupu do funkcie manažéra KB
Dátum určenia do funkcie manažéra KB
25.7.2021

C.3 Vyplýva z pozície Vami určeného manažéra KB jeho možnosť predkladať návrhy a oznamovať informácie v oblasti KB priamo štatutárnemu orgánu danej PZS a jeho nezávislosť od riadenia prevádzky a vývoja služieb informačných technológií?
Preukázanie dodržania primeraného postavenia manažéra KB potrebného pre riadny výkon funkcie vymedzené podľa § 5 písm. a) vyhlášky č. 362/2018 Z. z.?
áno

Časť D: Informačné systémy

Identifikácia centrálnych informačných systémov, ktoré tvoria jednu zo základných služieb, popis ich funkčnosti a ich kategória podľa vyhlášky č. 362/2018 Z. z. V prípade, že má Vaša organizácia viac ako 5 informačných systémov, použite prosím priloženú prílohu "Formulár pre dodatočné informačné systémy" na odovzdanie zvyšných IS.
(§20 ods. 2 zákona č. 69/2018 Z. z. a § 4 ods. 6 vyhlášky č. 362/2018 Z. z.)
IS = Informačný systém
ZS = Základné služby

D.1 Názov centrálneho IS podporujúceho ZS
Názov centrálneho IS, ktorý tvorí samostatný funkčný a technologický celok vykonávajúci špecifické procesy alebo služby, ktoré podporujú ZS.
LABmeter

D.3 Názov ZS, ktorú podporuje
Výber ZS, ktorú uvedený IS podporuje
Laboratórne služby

D.4 Kategória IS
Podľa metodiky v prílohe č. 2 k vyhláške č. 362/2018 Z.z.
Kat. II.

Časť E: Stratégia KB

Informácia o tom, či je vedením prijatá stratégia kybernetickej bezpečnosti ako dokument určujúci hlavné ciele prevádzkovateľa základnej služby v oblasti ďalšieho rozvoja kybernetickej bezpečnosti.
(§ 3 vyhlášky NBÚ č. 362/2018 Z.z.)
KB = Kybernetická bezpečnosť

E.1 Máte manažmentom prijatú stratégiu kybernetickej bezpečnosti a jej príslušné ciele?
Stratégia obsahuje minimálne určenie cieľov KB, všeobecné zodpovednosti a povinnosti v oblasti KB pri ich napĺňaní.
áno

Časť F: Správa aktív

Popis toho ako má prevádzkovateľ identifikované svoje aktíva (informácie, procesy, HW, SW, služby, sieťové komponenty a dodávateľov) ako základný stavebný prvok základných služieb a ako je prevádzkovateľ ZS schopný spravovať ich počas prevádzky základnej služby.
(§ 20 ods. 3 písm. b) zákona č. 69/2018 Z.z. a § 6 vyhlášky č. 362/2018 Z.z.)
Informačné aktíva (angl. „information assets“) = pojem používaný pre označenie širokej skupiny komponentov informačnej architektúry. Informačným aktívom môže byť každá informácia, systém, aplikácia alebo hardvér v majetku organizácie, ktorý sa používa pri prevádzkových činnostiach. Záleží len od vlastníkov alebo štatutárneho vedenia organizácie, do akého detailu bude evidovať tento svoj informačný majetok.
HW = Hardware
SW = Software
ZS = Základné služby

F.1 Máte identifikované všetky informačné aktíva, ktoré podporujú niektorú z identifikovaných ZS?
Informačné aktíva sú dáta a informácie spracúvané v IS a sú esenciálnou súčasťou poskytovania ZS.
áno

F.2 Máte určenú ich klasifikáciu pre dôvernosť, integritu a dostupnosť?
Podľa metodiky v prílohe č. 2 k vyhláške č. 362/2018 Z. z.
áno

F.3 Máte identifikované všetky podporné aktíva, ktoré podporujú niektorú z identifikovaných ZS?
Podporné aktíva sú všetky HW a SW prvky a služby, ktoré zabezpečujú spracovanie informačných aktív.
áno

F.4 Máte identifikovaných všetkých dodávateľov, ktorí Vám svojím poskytovaním služieb podporujú prevádzku ZS?
Dodávateľom podporujúcim ZS je každý externý subjekt, ktorého výpadok v dodávke služby spôsobí obmedzenie alebo výpadok prevádzky ZS.
áno

F.5 Máte identifikovaných vlastníkov ku všetkým identifikovaným aktívam?
Vlastník informačného alebo podporného aktíva je rola, ktorá zabezpečí, že bude aktívum riadne identifikované, a manažované počas celého svojho životného cyklu.
áno

F.6 Vediete si evidenciu všetkých aktív podieľajúcich sa na prevádzke ZS?
Evidencia aktív s uvedením jednoznačnej identifikácie aktíva, jeho logického a fyzického umiestnenia, jeho vlastníka a správcu počas celého životného cyklu aktíva.
áno

F.5 Máte zavedený proces na aktualizáciu evidencie aktív?
Proces musí mať aspoň definovaný postup a role a zodpovednosti namapované na pozície v organizačnej štruktúre.
áno

Časť G: Manažment konfigurácií

Popis toho aký má prevádzkovateľ prehľad o nastaveniach svojich aktív a o evidencii zmien týchto nastavení.
(§ 20 ods. 3 písm. g) zákona č. 69/2018 Z.z. a § 6 vyhláška č. 362/2018 Z. z.)
Konfiguračné nastavenia = Špecifické nastavenia aplikačného softvéru, komponentu, informačného systému, resp. iného objektu zabezpečujúceho službu
Aktíva = Informácie, procesy, HW, SW, služby, sieťové komponenty a dodávateľov

G.1 Vediete si evidenciu o konfiguračných nastaveniach identifikovaných aktív a služieb?
Evidencia by mala obsahovať jednoznačnú identifikáciu aktíva, jej konfiguračných nastavení, dátum poslednej verzie nastavení a identifikáciu zodpovedného pracovníka za uvedený záznam.
áno

G.2 Máte zavedený proces pravidelného aktualizovania záznamov v evidencii konfigurácií aktív a služieb?
Proces musí mať aspoň definovaný postup a role a zodpovednosti namapované na pozície v organizačnej štruktúre.
áno

Časť H: Technické zraniteľnosti

Popis toho ako je prevádzkovateľ schopný identifikovať či sa publikované známe zraniteľnosti týkajú jeho aktív a schopnosť vyhodnocovať riziko potenciálneho prieniku zneužitím týchto zraniteľností.
(§ 20 ods. 3 písm. g) zákona č. 69/2018 Z. z. a § 9 vyhlášky NBÚ č. 362/2018 Z. z.)
Zraniteľnosť (Vulnerability) = Pojem používaný v riadení rizík pre označenie slabiny či nedostatku aktíva. Zraniteľnosť umožňuje uplatnenie hrozby.
Aktíva = Informácie, procesy, HW, SW, služby, sieťové komponenty a dodávateľov

H.1 Získavate informácie o známych zraniteľnostiach od dodávateľov Vašich aktív, SK-CERT, CSIRT-SK, prípadne iných?
Notifikácie o známych zraniteľnostiach by mal prevádzkovateľ získavať aspoň od výrobcov všetkých svojich zariadení, SK-CERT alebo CSIRT-SK, prípadne iných relevantných zdrojov.
áno

H.2 Vyhodnocujete dopad známych zraniteľností na Vaše aktíva a vyhodnocujete riziko spojené s týmito zraniteľnosťami?
Po získaní informácie o známej zraniteľnosti je potrebné vyhodnocovať, či a aký má daná zraniteľnosť dopad na dotknuté aktívum a rozhodnúť o ďalšom postupe na základe výsledkov analýzy rizík.
áno

Časť I: Prevádzkový monitoring

Schopnosť prevádzkovateľa identifikovať a vyhodnocovať stavové veličiny svojich aktív tak, aby bol schopný odhaliť potenciálne zlyhanie konkrétneho prvku alebo celej služby.
(§ 20 ods. 3 písm. k) zákon č. 69/2018 Z. z. a § 15 vyhlášky č. 362/2018 Z.z.)
Aktíva = Informácie, procesy, HW, SW, služby, sieťové komponenty a dodávateľov
Stavová veličina = veličina charakterizujúca stav daného aktíva (napr. doba prevádzky, poruchovosť)

I.1 Máte určené, pre ktoré aktíva a komponenty vo Vašom prostredí potrebujete mať nastavený prevádzkový monitoring?
Presne určené a identifikované aktíva a ich parametre, ktoré potrebujete monitorovať.
áno

I.2 Vykonávate monitoring týchto parametrov tak, aby ste mali nepretržitý prehľad o Vašom prostredí?
Vykonávate aktívny zber stavových záznamov zo všetkých určených aktív s dostatočnou retenčnou dobou a zabezpečením nezmeniteľnosti týchto záznamov?
áno

Časť J: Bezpečnostný monitoring

Schopnosť prevádzkovateľa identifikovať také udalosti (za normálnej prevádzky bežné) alebo kombináciu udalostí v jeho infraštruktúre, ktoré môžu znamenať prítomnosť škodlivého kódu alebo hackera.
(§20 ods. 3 písm. k) zákona č. 69/2018 Z. z. a § 15 vyhlášky č. 362/2018 Z.z.)

J.1 Máte implementovaný nástroj na výkon bezpečnostného monitoringu nad aktívami, ktoré sa podieľajú na základnej službe?
Nástroj, ktorý je schopný vyhodnocovať bezpečnostné udalosti na základe detegovaných stavových záznamov získaných z definovaných aktív a identifikáciu potenciálnych kybernetických bezpečnostných incidentov.
áno

J.2 Máte nastavený proces, ktorým budete vedieť reagovať na kybernetický bezpečnostný incident?
Proces musí mať aspoň definovaný postup a role a zodpovednosti namapované na pozície v organizačnej štruktúre.
áno

Časť K: Personálna bezpečnosť

Popis toho ako vykonáva prevádzkovateľ kontrolu dodržiavania svojich politík vlastnými zamestnancami alebo zamestnancami dodávateľov.
(§ 20 ods. 3 písm. c) zákona č. 69/2018 Z.z. a § 7 vyhlášky č. 362/2018 Z. z.)

K.1 Vykonávate kontrolu dodržiavania bezpečnostných politík zo strany vlastných zamestnancov a zamestnancov dodávateľov?
Viesť evidenciu rozsahu a termínu zaškolenia bezpečnostných politík KB vlastných zamestnancov a zamestnancov dodávateľa a viesť evidenciu kontroly ich dodržiavania.
áno

Časť L: Riadenie rizík

Schopnosť prevádzkovateľa identifikovať riziká kybernetickej bezpečnosti, vyhodnotiť ich veľkosť a navrhnúť k nim opatrenia na zníženie rizika.
(§ 20 ods. 3 písm. b) zákona č. 69/2018 Z.z. a § 6 vyhlášky č. 362/2018 Z. z.)

L.1 Identifikujete a vyhodnocujete riziká kybernetickej bezpečnosti?
Analýzu rizík vykonávate s ohľadom na zraniteľnosti, hrozby, aktíva, existujúce bezpečnostné opatrenia, mieru akceptovaného rizika a funkčnej analýzy dopadu podľa niektorej zo štandardných metodík (napr. ISO/IEC 27005).
áno

L.2 Navrhujete a implementujete bezpečnostné opatrenia kybernetickej bezpečnosti, ktorými znížite neakceptovateľne veľké zvyškové riziká?
Evidencia navrhovaných opatrení v súvislosti s neakceptovateľne vysokými rizikami KB a priebežne aktualizovaný plán ich implementácie.
áno

Časť M: Riadenie bezpečnosti sietí

Popis toho aký je stav a spôsob správy sieťovej segmentácie a zariadení, ktoré segmentáciu zabezpečujú v prostredí prevádzkovateľa.
(§ 20 ods. 3 písm. f) zákona č. 69/2018 Z.z. a § 10 vyhlášky č. 362/2018 Z. z.)
Segmentácia sietí = vytvorenie podsiete v rámci podnikovej siete alebo nejakého iného typu celkovej počítačovej siete. Segmentácia siete umožňuje zamedziť výskytu škodlivého softvéru a iných hrozieb a môže zvýšiť efektívnosť z hľadiska výkonu siete, napr. umiestnenie vnútorného firewallu v sieti.

M.1 Máte implementovanú bezpečnostnú sieťovú segmentáciu?
Definované pravidlá pre jednotlivé sieťové segmenty, evidenciu aktív umiestnených v jednotlivých segmentoch a nastavenú pravidelnú kontrolu dodržiavania danej segmentácie.
áno

M.2 Vykonávate aktívnu a priebežnú správu pravidiel na zariadeniach oddeľujúcich jednotlivé sieťové segmenty?
Evidencia všetkých pravidiel sieťového prestupu medzi segmentami, nastavený a pravidelne vykonávaný kontrolný mechanizmus, ktorý porovná reálne nastavené pravidlá s vedenou evidenciou.
áno

Časť N: Riadenie prístupov

Popis toho ako prevádzkovateľ riadi prístupy vlastných používateľov a používateľov dodávateľov ku svojim informáciám, zariadeniam a sieťam.
(§ 20 ods. 3 písm. d) zákona č. 69/2018 Z.z. a vyhláška č. 362/2018 Z. z.)

N.1 Máte definované rozsahy logických a aj fyzických prístupových oprávnení vlastných zamestnancov a zamestnancov dodávateľov ku všetkým svojim aktívam?
Sú definované role a k nim prislúchajúce rozsahy oprávnení s rešpektovaním minimálne týchto zásad: zásada najnižších privilégií "least privilege", zásada sprístupnenia tých prostriedkov, ktoré sú nevyhnutné k práci "need-to-do", zásada oddelenia zodpovednosti "segregation of duties" a v riadení prístupov sú použité jednoznačné identifikátory identít.
áno

N.2 Vykonávate pravidelnú kontrolu nad nastavenými rozsahmi prístupových oprávnení na Vašich aktívach?
Evidencia všetkých pridelených privilégií, nastavený a pravidelne vykonávaný kontrolný mechanizmus, ktorý porovná reálne nastavené prístupy s vedenou evidenciou.
áno

Časť O: Riadenie procesov pre správu a údržbu IS

Popis toho ako prevádzkovateľ vykonáva správu svojich zariadení a systémov v prevádzke a ako je schopný udržať ich v riadnom chode.
(§ 20 ods. 3 písm. f) zákona č. 69/2018 Z.z. a § 11 vyhlášky č. 362/2018 Z. z.)
IS = Informačný systém

O.1 Máte zavedený proces zmenového konania (Change management)?
Proces musí mať definované aspoň typy zmien, procesné aktivity, role a zodpovednosti, ktoré sú namapované na pozície v organizačnej štruktúre.
áno

O.2 Máte zavedený proces incident manažmentu?
Proces musí mať definované aspoň procesné aktivity, role a zodpovednosti, ktoré sú namapované na pozície v organizačnej štruktúre.
áno

O.3 Máte zavedený proces zálohovania?
Proces musí mať definované presné postupy, role a zodpovednosti, ktoré sú namapované na pozície v organizačnej štruktúre.
áno

O.4 Máte zavedený proces kontinuity procesov a služieb a obnovu po havárii?
Proces musí mať identifikované kľúčové procesy v spoločnosti, scenáre typov havárií, postupy pre obnovu kľúčových procesov, definované role a zodpovednosti, ktoré sú namapované na pozície v organizačnej štruktúre.
áno

Časť P: Riadenie dodávateľských vzťahov

Schopnosť prevádzkovateľa zadefinovať požiadavky na dodávateľa pred zmluvným vzťahom a aj schopnosť ich merať a vyhodnocovať počas prevádzky.
(§ 20 ods. 3 písm. e) zákona č. 69/2018 Z.z. a § 8 vyhlášky č. 362/2018 Z. z.)
SLA = Service-level agreement (Dohoda o úrovni poskytovaných služieb)

P.1 Monitorujete na pravidelnej báze parametre služieb, ktoré Vám poskytujú dodávatelia?
Definované SLA parametre, stanovený spôsob ich monitorovania a vyhodnocovanie odchýlok daných parametrov.
áno

Bezpečnostné opatrenia podľa zákona č. 69/2018 Z. z.

§ 20

Bezpečnostné opatrenia

(1) Bezpečnostnými opatreniami na účely tohto zákona sú úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov. Bezpečnostné opatrenia realizované v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov a v súlade s bezpečnostnými štandardmi v oblasti kybernetickej bezpečnosti sa prijímajú s cieľom predchádzať kybernetickým bezpečnostným incidentom a minimalizovať vplyv kybernetických bezpečnostných incidentov na bezpečnosť prevádzkovania služby. Bezpečnostné opatrenia sú všeobecné, realizované v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov a v súlade s bezpečnostnými štandardmi v oblasti kybernetickej bezpečnosti pre všetky siete a informačné systémy a sektorové, ktoré sa realizujú na základe špecifík kategorizácie sietí a informačných systémov ústredného orgánu v rozsahu svojej pôsobnosti podľa prílohy č. 1 a v súlade s bezpečnostnými štandardmi v oblasti kybernetickej bezpečnosti.

(2) Klasifikácia informácií a kategorizácia sietí a informačných systémov podľa odseku 1 sa vykonáva na základe významnosti, funkcie a účelu informácií a informačných systémov s ohľadom na dôvernosť, integritu, dostupnosť, kvalitu služby a kontrolnú činnosť.

(3) Bezpečnostné opatrenia sa prijímajú a realizujú najmä pre oblasť

a) organizácie kybernetickej bezpečnosti a informačnej bezpečnosti,
b) riadenia rizík kybernetickej bezpečnosti a informačnej bezpečnosti,
c) personálnej bezpečnosti,
d) riadenia prístupov,
e) riadenia kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami,
f) bezpečnosti pri prevádzke informačných systémov a sietí,
g) hodnotenia zraniteľností a bezpečnostných aktualizácií,
h) ochrany proti škodlivému kódu,
i) sieťovej a komunikačnej bezpečnosti,
j) akvizície, vývoja a údržby informačných sietí a informačných systémov,
k) zaznamenávania udalostí a monitorovania,
l) fyzickej bezpečnosti a bezpečnosti prostredia,
m) riešenia kybernetických bezpečnostných incidentov,
n) kryptografických opatrení,
o) kontinuity prevádzky,
p) auditu, riadenia súladu a kontrolných činností.

(4) Bezpečnostné opatrenia musia zahŕňať najmenej

a) určenie manažéra kybernetickej bezpečnosti, ktorý je pri návrhu, prijímaní a presadzovaní bezpečnostných opatrení nezávislý od štruktúry riadenia prevádzky a vývoja služieb informačných technológií a ktorý spĺňa znalostné štandardy pre výkon roly manažéra kybernetickej bezpečnosti,
b) detekciu kybernetických bezpečnostných incidentov,
c) evidenciu kybernetických bezpečnostných incidentov,
d) postupy riešenia a riešenie kybernetických bezpečnostných incidentov,
e) určenie kontaktnej osoby pre prijímanie a evidenciu hlásení,
f) pripojenie do komunikačného systému pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálneho systému včasného varovania.

(5) Bezpečnostné opatrenia sa prijímajú a realizujú na základe analýzy rizík kybernetickej bezpečnosti, ktorá určuje pravdepodobnosť vzniku škodlivej udalosti. Súčasťou analýzy rizík je aj analýza politického rizika tretej strany, pričom politické riziko sa posudzuje najmä vzhľadom na:

a) plnenie záväzkov z medzinárodných zmlúv, ktorými je Slovenská republika viazaná, a na jej členstvo v medzinárodných organizáciách,
b) možnosť ovplyvňovania a zasahovania do činnosti tretej strany štátom, ktorý nie je členským štátom Európskej únie a Organizácie Severoatlantickej zmluvy (ďalej len „cudzí štát“),
c) analýzu vlastníckej štruktúry a riadiacej štruktúry tretej strany vrátane vlastníckeho podielu
cudzieho štátu a priamych zahraničných investícií do tretej strany,
d) analýzu právnych predpisov a medzinárodných záväzkov cudzieho štátu v oblasti ochrany
základných ľudských práv a slobôd, kybernetickej bezpečnosti, boja proti počítačovej kriminalite, ochrany osobných údajov a ochrany informácií,
e) informácie špecifické pre cudzí štát a informácie spravodajskej služby o možných hrozbách pre záujmy Slovenskej republiky. Politické riziká schvaľuje vláda Slovenskej republiky na základe stanoviska úradu. Stanovisko úradu sa predkladá Bezpečnostnej rade Slovenskej republiky. Politické riziká úrad zverejňuje v jednotnom informačnom systéme kybernetickej bezpečnosti. Úrad v analýze politického rizika zohľadní vyjadrenie Ministerstva zahraničných vecí a európskych záležitostí Slovenskej republiky, Ministerstva hospodárstva Slovenskej republiky, Ministerstva vnútra Slovenskej republiky, Slovenskej informačnej služby a Ministerstva obrany Slovenskej republiky z oblasti ich pôsobnosti.

(6) Bezpečnostné opatrenia sa prijímajú a realizujú na základe schválenej bezpečnostnej dokumentácie, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu.

(7) Povinnosť dodržiavať všeobecné bezpečnostné opatrenia a sektorové bezpečnostné opatrenia v rozsahu podľa tohto zákona a všeobecne záväzných právnych predpisov vydaných na jeho vykonanie sa vzťahuje aj na právne vzťahy, o ktorých tak ustanoví osobitný predpis.