NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

# Certifikačná schéma overovania odbornej spôsobilosti manažéra kybernetickej bezpečnosti

Verzia 1.0.7 zo dňa 29. apríla 2021

# 1 TERMÍNY A DEFINÍCIE

| Termín | Význam |
|---|---|
| akreditácia | atestácia treťou stranou týkajúca sa orgánu posudzovania zhody, ktorá slúži ako oficiálny dôkaz kompetentnosti plniť špecifické úlohy posudzovania zhody (ISO/IEC 17000: 2004) |
| atestácia | vydanie osvedčenia založeného na rozhodnutí po preskúmaní, že sa preukázalo splnenie určených požiadaviek (ISO/IEC 17000: 2004) |
| audit | systematický, nezávislý a zdokumentovaný proces získavania záznamov, konštatovaní faktov alebo iných dôležitých informácií a ich objektívneho posudzovania s cieľom určiť rozsah, v akom sa splnili určené požiadavky (ISO/IEC 17024:2012) |
| autorizácia | zmocnenie orgánu posudzovania zhody štátom vykonávať určené činnosti posudzovania zhody (ISO/IEC 17000: 2004) |
| certifikačné požiadavky | súbor stanovených požiadaviek, vrátane požiadaviek schémy, ktoré je potrebné splniť, na preukázanie alebo udržanie certifikácie (ISO/IEC 17024:2012) |
| certifikačný orgán | orgán vykonávajúci posudzovanie zhody treťou stranou podľa certifikačnej schémy (ISO/IEC 17024:2012) |
| certifikačný proces | činnosti, na základe ktorých certifikačný orgán určí, že osoba spĺňa certifikačné požiadavky , zahŕňa podanie žiadosti, posúdenie, rozhodnutie o certifikácii, recertifikácii a používanie certifikátov, loga a certifikačných značiek (ISO/IEC 17024:2012) |
| certifikát | dokument vydaný certifikačným orgánom v súlade s ustanoveniami tejto medzinárodnej normy, osvedčujúci, že menovaná osoba splnila certifikačné požiadavky (ISO/IEC 17024:2012) |
| dohľad | systematické opakovanie činností posudzovania zhody ako základ udržania platnosti stanoviska o zhode (ISO/IEC 17000: 2004) |
| dozor | osoba poverená certifikačným orgánom, ktorá pomáha dohliadať alebo dohliada na skúšku, ale nehodnotí kompetentnosť kandidáta |
| kandidát | žiadateľ, ktorý splnil stanovené predpoklady a bol zaradený do certifikačného procesu (ISO/IEC 17024:2012) |
| kvalifikácia | preukázané vzdelanie, odborná príprava a pracovné skúsenosti |
| objekt posudzovania zhody | akýkoľvek konkrétny materiál, produkt, inštalácia, proces, systém, osoba alebo orgán, ktorých sa týka posudzovanie zhody (ISO/IEC 17065: 2013, ISO/IEC 17021-1:2015, ISO/IEC 17024:2012) |
| odvolanie sa | žiadosť žiadateľa, kandidáta alebo certifikovanej osoby o opätovné zváženie akéhokoľvek rozhodnutia certifikačného orgánu, ktoré sa týka ním požadovaného stavu certifikácie (ISO/IEC 17024:2012) |
| orgán posudzovania zhody | orgán, ktorý vykonáva služby posudzovania zhody (ISO/IEC 17024:2012) |
| posudzovanie | proces, ktorým sa hodnotí ako konkrétna osoba splnila požiadavky certifikačnej schémy (ISO/IEC 17024:2012) |
| posudzovanie zhody | dokazovanie, že sa splnili určené požiadavky týkajúce sa produktu, procesu, systému, osoby alebo orgánu (ISO/IEC 17000: 2004) |
| skúšajúci | kompetentná osoba na vykonávanie a klasifikovanie skúšky ak skúška vyžaduje odborné hodnotenie |

| Termín | Význam |
|---|---|
| skúšanie (testovanie) | určenie jednej alebo viacerých charakteristík objektu posudzovania zhody podľa postupu. Termín skúšanie sa zvyčajne týka materiálov, produktov alebo procesov. V niektorých aplikačných oblastiach sa uprednostňuje z angličtiny prevzatý termín testovanie, resp. test (napr. testovanie hypotéz, testovanie softvéru a pod.). (ISO/IEC 17000: 2004) |
| skúška | mechanizmus, tvoriaci časť posudzovania ktorým sa hodnotí kompetentnosť kandidáta jedným alebo viacerými spôsobmi, ako písomne, ústne, prakticky alebo pozorovaním, podľa nadefinovania v certifikačnej schéme |
| spôsobilosť | schopnosť uplatniť vedomosti a zručnosti na dosiahnutie zamýšľaných výsledkov |
| sťažnosť | vyjadrenie nespokojnosti, inej ako v odvolaní, predložené certifikačnému orgánu jednotlivcom alebo organizáciou, vo veci činností tohto orgánu alebo certifikovanej osoby, s očakávaním odpovede (ISO/IEC 17024:2012) |
| špecifikácia spôsobilostí | normatívny dokument definujúci kritériá spôsobilosti |
| vlastník schémy | organizácia zodpovedná za rozvoj a udržiavanie certifikačnej schémy (ISO/IEC 17024:2012) |
| žiadateľ | osoba, ktorá podala žiadosť o prijatie do certifikačného procesu (ISO/IEC 17024:2012) |

# 2 ÚVOD

## 2.1 ROZSAH CERTIFIKÁCIE

| | |
|---|---|
| Predmet certifikácie | Manažér kybernetickej bezpečnosti podľa osobitných predpisov[1) 2] |
| Opis práce a úloh | Plánovanie, riadenie implementácie, prevádzka a udržiavanie bezpečnostných opatrení a plnenie požiadaviek ustanovených Zákonom o kybernetickej bezpečnosti, Zákonom o informačných technológiách vo verejnej správe a ich vykonávacími predpismi |

## 2.2 PRÁVNY ZÁKLAD A NORMATÍVNE KRITÉRIÁ

Táto certifikačná schéma sa opiera najmä o nasledovné právne úpravy a technické normy:

- Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov
- Zákon č. 95/2019 Z.z. informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov
- Vyhláška NBÚ č. 362/2018 Z.z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení
- Vyhláška ÚPVII č. 179/2020 Z. z. ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy
- Zákon č. 56/2018 Z.z. o posudzovaní zhody výrobku, sprístupňovaní určeného výrobku na trhu a o zmene a doplnení niektorých zákonov
- ISO/IEC 17024:2012 Posudzovanie zhody - Všeobecné požiadavky na orgány vykonávajúce certifikáciu osôb
- ISO/IEC 17000:2020 Posudzovanie zhody - Slovník a všeobecné zásady

Pokiaľ nie je uvedená verzia dokumentu, všetky vyššie uvedené právne predpisy a technické normy sú citované v znení ich platnej verzie.

## 2.3 CERTIFIKAČNÉ ROLY

### 2.3.1 Vlastník certifikačnej schémy

Certifikačnú schému overovania odbornej spôsobilosti manažéra vydáva **Národný bezpečnostný úrad**, ako orgán dohľadu v oblasti kybernetickej bezpečnosti. Certifikačná schéma poskytuje postup pri certifikácii manažéra kybernetickej bezpečnosti podľa osobitného predpisu[1)].

### 2.3.2 Orgány posudzovania zhody

V záujme zachovania kvality určuje certifikačná schéma certifikačné procesy, všeobecné a osobitné požiadavky na certifikáciu manažéra kybernetickej bezpečnosti. Služby posudzovania zhody vykonávajú **orgány posudzovania zhody** podľa tejto certifikačnej schémy a podľa odporúčaní medzinárodne akceptovaných štandardov alebo iných vecne obdobných postupov[3]) príslušným na certifikáciu personálu.

Orgán posudzovania zhody vydávajúci certifikáty založené na tejto certifikačnej schéme musí spĺňať požiadavky normy ISO/IEC 17024.

Orgán posudzovania zhody je oprávnený vydávať certifikát manažéra kybernetickej bezpečnosti podľa osobitného predpisu[1)]

[1)] § 5 ods. 1 písm. a) Vyhlášky NBÚ č. 362/2018 Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení

[2)]Príloha č. 2 k vyhláške ÚPVII č. 179/2020 Z. z. ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy

### 2.3.3 Akreditačný orgán

Vnútroštátny **akreditačný orgán** je jediný orgán v členskom štáte EÚ, ktorý vykonáva akreditáciu na základe právomoci, ktorú mu udelil štát. V Slovenskej republike je vnútroštátnym akreditačným orgánom Slovenská národná akreditačná služba (SNAS). Postavenie SNAS a jej pôsobnosť určuje zákon č. 505/2009 Z. z. o akreditácii orgánov posudzovania zhody a o zmene a doplnení niektorých zákonov.

SNAS v zmysle politiky PL-45 Vydávanie certifikátov certifikačnými orgánmi na certifikáciu osôb v neakreditovanom režime nariaďuje orgánom posudzovania zhody na certifikáciu osôb zákaz vydávania neakreditovaných certifikátov v rozsahoch, ktoré sú pokryté akreditáciou SNAS. Pod pojmom neakreditovaný certifikát sa rozumie certifikát, ktorý neobsahuje akreditačnú značku a / alebo odkaz na akreditáciu.

Vzhľadom na to, že ku dňu účinnosti tejto certifikačnej schémy certifikácia manažéra kybernetickej bezpečnosti nie je pokrytá akreditáciou SNAS, orgán posudzovania zhody je na základe výnimky SNAS oprávnený vydávať certifikát manažéra kybernetickej bezpečnosti pre oblasť certifikácie manažérov v súlade s touto certifikačnou schémou. V prípade rozšírenia akreditácie podľa normy ISO/IEC 17024: 2012, bude certifikačný orgán povinný certifikáty manažérov kybernetickej bezpečnosti podľa osobitného predpisu[1)], vydané v neakreditovanom režime opätovne vydať, v lehote najneskôr do jedného roka od dátumu rozhodnutia o udelení akreditácie Slovenskou národnou akreditačnou službou[3)] pre oblasť certifikácie manažérov.

[3] ) § 9 zákona č. 505/2009 Z. z. o akreditácii orgánov posudzovania zhody a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

# 3 KRITÉRIÁ CERTIFIKÁCIE

## 3.1 VŠEOBECNÉ POŽIADAVKY NA SPÔSOBILOSŤ

### 3.1.1 Minimálne všeobecné požiadavky na spôsobilosť

Od kandidáta sa vyžaduje znalosť v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti, riadenia IT služieb a správy informačných systémov, prípadne doložená ekvivalentným osvedčením o odbornej spôsobilosti, doložené medzinárodne platným certifikátom. Kandidát musí byť schopný analyzovať a riadiť systém manažérstva informačnej bezpečnosti v súlade s príslušnými technickými normami a právnymi predpismi a aplikovať príslušné metódy riadenia.

### 3.1.2 Minimálne požiadavky na vzdelanie a prax

Minimálne požiadavky na úroveň vzdelania a prax žiadateľa o overenie odbornej spôsobilosti:

| Vzdelanie a požadovaný doklad | Prax a spôsob jej preukázania (alternatívy predložených dokumentov) |
|---|---|
| Úplné stredné všeobecné vzdelanie a úplné stredné odborné vzdelanie (doklad o získanom stupni vzdelania a o získanej kvalifikácii) | • skúsenosti v oblasti informačných technológií - najmenej **10 rokov praxe** (životopis s uvedením kontaktu na overiteľnú referenciu),<br>• skúsenosti v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT - najmenej **7 rokov praxe**<br>• medzinárodný certifikát z oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT sa považuje za započítateľnú odbornú prax (nepovinný, nahrádza 3 roky praxe) |
| Vysokoškolské vzdelanie prvého stupňa (doklady o absolvovaní štúdia) | • skúsenosti v oblasti informačných technológií - najmenej **7 rokov praxe** (životopis s uvedením kontaktu na overiteľnú referenciu),<br>• skúsenosti v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT - najmenej **5 rokov praxe**<br>• medzinárodný certifikát z oblasti riadenia informačnej bezpečnosti sa považuje započítateľnú odbornú prax (nepovinný, nahrádza 3 roky praxe) |
| Vysokoškolské vzdelanie druhého stupňa (doklady o absolvovaní štúdia) | • skúsenosti v oblasti informačných technológií - najmenej **5 rokov praxe** (životopis s uvedením kontaktu na overiteľnú referenciu),<br>• skúsenosti v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT - najmenej **3 roky praxe**<br>• medzinárodný certifikát z oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT sa považuje za odbornú prax (nepovinný, nahrádza 3 roky praxe) |

### 3.1.3 Všeobecné predpoklady na výkon činnosti manažéra

Uchádzačom sa môže stať fyzická osoba, ktorá:

- má spôsobilosť na právne úkony v plnom rozsahu,
- je bezúhonná (môže sa vyžadovať doloženie výpisu z registra trestov nie staršieho ako 3 mesiace),
- spĺňa všeobecné a osobitné požiadavky na spôsobilosť,

- je oprávnená na oboznamovanie sa s utajovanými skutočnosťami podľa osobitného predpisu, ak sa takéto oprávnenie na dohodnutú prácu vyžaduje.

### 3.1.4 Osobnostné predpoklady na výkon činnosti manažéra

Od kandidáta sa vyžadujú nasledujúce osobnostné požiadavky a schopnosti:

- prijímať rozhodnutia,
- myslieť a konať holisticky,
- rozpoznať a komunikovať význam a hodnotu faktov,
- riadiť zmeny,
- riešiť konflikty,
- poskytovať spätnú väzbu,
- delegovať úlohy,
- podporovať procesy vzdelávania a odovzdávania znalostí,
- viesť pracovný tím.

## 3.2 OSOBITNÉ POŽIADAVKY NA SPÔSOBILOSŤ

Od kandidáta sa vyžadujú nasledujúce minimálne požiadavky (znalosti, schopnosti, zručnosti) na úroveň odbornej spôsobilosti manažéra pre proces riadenia kybernetickej bezpečnosti:

1. Znalosť procesov a systému riadenia informačnej a kybernetickej bezpečnosti
2. Znalosť zásad organizácie informačnej a kybernetickej bezpečnosti
3. Znalosť zásad personálnej bezpečnosti
4. Znalosť zásad riadenia prístupov a identít
5. Znalosti o spôsobe používania kryptografických bezpečnostných mechanizmov
6. Znalosť princípov testovania kybernetickej bezpečnosti
7. Znalosť právnych predpisov, požiadaviek na súlad a noriem vzťahujúcich sa na kybernetickú bezpečnosť, najmä:
    - smernice Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii,
    - nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti)
    - nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu,
    - zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti a o doplnení niektorých zákonov,
    - vyhlášky NBÚ č. 362/2018 Z.z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení,
    - vyhlášky NBÚ č. 164/2018 Z. z. ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby),
    - vyhlášky NBÚ č. 165/2018 Z. z. ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov,
    - vyhlášky NBÚ č. 166/2018 Z. z. o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov,
    - zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o doplnení niektorých zákonov,

- vyhlášky ÚPVII č. 179/2020 Z. z. ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy,
- zákona č. 45/2011 Z. z. o kritickej infraštruktúre,
- zákona č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách),
- medzinárodných noriem rady ISO/IEC 27000 „Informačné technológie - Bezpečnostné metódy - Systémy riadenia informačnej bezpečnosti“,
- medzinárodných noriem rady ISA/IEC 62443 „Security for Industrial Automation and Control Systems“ ak sa takáto znalosť na dohodnutú prácu vyžaduje.

8. Znalosť právnych predpisov a požiadaviek na súlad vzťahujúcich sa na ochranu osobných údajov, najmä:
   - nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
   - zákona č. 18/2018 Z. z. o ochrane osobných údajov a o doplnení niektorých zákonov,
   - smernice Európskeho parlamentu a Rady2002/58/ES z 12. júla 2002, týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) a jej implementácie v zákone č. 351/2011 Z. z. o elektronických komunikáciách
9. Znalosť štandardov a zásad ochrany osobných údajov, vrátane metodických usmernení Úradu na ochranu osobných údajov Slovenskej republiky a Výboru na ochranu údajov (EÚ)
10. Schopnosť navrhovať a uplatniť bezpečnostné stratégie a politiky
11. Znalosť procesov a metodík riadenia rizík
12. Znalosť postupov analýzy rizík
13. Znalosť typických hrozieb a postupov pre identifikáciu hrozieb a zraniteľností
14. Znalosť bezpečnostných mechanizmov
15. Znalosť princípov podnikovej architektúry, orientácia v architektúrnych rámcoch
16. Znalosť procesov riešenia kybernetických bezpečnostných incidentov
17. Znalosť princípov plánovania havarijnej obnovy prevádzky
18. Znalosť procesov riadenia kontinuity činností
19. Znalosť metód posudzovania rizík a schopnosť ich aplikovať v rámci organizácie
20. Schopnosť analyzovať a kvantifikovať riziká
21. Schopnosť analyzovať a hodnotiť bezpečnostné mechanizmy a riešenia

# 4 POSÚDENIE ZHODY

## 4.1 POČIATOČNÉ KRITÉRIÁ CERTIFIKÁCIE

Posúdenie spôsobilosti kandidátov podľa tejto schémy má za cieľ overiť a potvrdiť, že boli dosiahnuté požiadavky na kvalifikáciu manažéra podľa osobitného predpisu s príslušnými spôsobilosťami, ktoré umožnia manažérom samostatne riadiť kybernetickú bezpečnosť v organizácii, riadiť implementáciu a udržiavanie opatrení v súlade s požiadavkami Vyhlášky NBÚ č. 362/2018 Z.z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení ako aj Vyhlášky ÚPVII č. 179/2020 Z. z. ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.

Ako predpoklad počiatočnej certifikácie musí orgán posudzovania zhody vyžadovať objektívne dôkazy o tom, že osoba, ktorá žiada o certifikáciu, spĺňa základné požiadavky týkajúce sa profilu uvedené v príslušnej špecifikácii spôsobilosti. Každý orgán posudzovania zhody je zodpovedný za identifikáciu vhodných referenčných úrovní v rámci príslušného kontextu národnej kvalifikácie a odbornej prípravy.

Predpoklady počiatočnej certifikácie zahŕňajú najmä:

- príslušné vzdelanie
- prax a rozsah všeobecných pracovných skúseností
- formálne školenia a odborné certifikáty
- manažérske skúsenosti
- plnenie požiadaviek kódexu profesionálneho správania manažéra kybernetickej bezpečnosti (etický kódex)

v kontexte systému hodnotenia a certifikácie riadeného v súlade s pravidlami akreditačného orgánu v členskom štáte EÚ, pod dohľadom akreditačného orgánu členského štátu.

Osvedčenia, ktorými je potvrdená atestácia splnenia všetkých týchto podmienok, sa na účely tejto schémy nazývajú „certifikáty“.

## 4.2 POSUDZOVANIE UCHÁDZAČOV

Posúdenie sa vykonáva plánovaným a štruktúrovaným spôsobom, ktorý zabezpečí, aby požiadavky schémy boli objektívne a systematicky overené a boli písomné dokumentované dôkazy potvrdzujúce kompetentnosť kandidáta.

Vlastník certifikačnej schémy priebežne overuje účinnosť metód na posudzovanie kandidátov. Týmto overením sa zabezpečí, aby každé posúdenie bolo spravodlivé a platné.

Konkrétne hodnotiace kritériá a metódy, ktoré sa majú použiť, vrátane druhov hodnotenia, s cieľom preukázať, že sa dosiahli požadované ciele môžu byť predmetom samostatných metodických usmernení vlastníka certifikačnej schémy.

## 4.3 ODBORNÁ SKÚŠKA

### 4.3.1 Obsah odbornej skúšky

Odborná skúška manažéra kybernetickej bezpečnosti sa vykonáva zo znalosti všeobecne záväzných právnych predpisov upravujúcich kybernetickú bezpečnosť a ochranu kritickej infraštruktúry v kontexte informačných a komunikačných technológií a oblastí spôsobilostí uvedených v kapitole 3.2.

Odborná skúška je vykonávaná formou testu obsahujúceho 100 otázok zo znalosti všeobecne záväzných právnych predpisov a príslušných technických noriem o podmienkach výkonu činnosti manažéra kybernetickej bezpečnosti a o bezpečnostných opatreniach v kybernetickej bezpečnosti. Konkrétny rozsah otázok je riešený v nasledujúcom článku tejto schémy.

Pre každú skúšku sa vygeneruje **100 otázok** náhodným výberom zo súboru obsahujúceho najmenej **300 otázok** schválených vlastníkom certifikačnej schémy.

Návrh každej skúšobnej otázky obsahuje:

a) znenie skúšobnej otázky, alebo príkladu s jednoznačným zadaním úlohy
b) návrh štyroch alternatívnych odpovedí pre danú otázku, z ktorých len jedna odpoveď môže byť správna
c) označenie správnych a nesprávnych odpovedí
d) vymedzenie odbornej domény, do ktorej príslušný návrh otázky patrí
e) návrh bodového ohodnotenia otázky
f) voliteľne – komentár ku spôsobu riešenia navrhnutej otázky

Každá otázka má 4 možností odpovedí, pričom správna je len jedna odpoveď. **Časový rozsah skúšky na 100 otázok je 150 minút** (t.j. 1,5 min./otázka).

Národný bezpečnostný úrad ako vlastník certifikačnej schémy na svojom webovom sídle zverejňuje:

a) okruhy a príklady otázok na vykonanie odbornej skúšky a usmernenie na ich používanie,
b) vzor žiadosti o vykonanie odbornej skúšky a
c) vzor certifikátu manažéra kybernetickej bezpečnosti.

### 4.3.2 Požiadavky na skúšobné otázky

- Každý orgán posudzovania zhody uchováva skúšobné otázky / prípadové štúdie / scenáre pre potreby odbornej skúšky. Štruktúra a obsah množiny otázok sa vzťahuje na vedomosti a zručnosti definované v platnej špecifikácii spôsobilostí.

Pre každú odbornú skúšku musí byť k dispozícii trojnásobný počet otázok vybratých pre skúšku. Otázky musia byť vyberané tak, aby sa zabezpečila nezávislosť jednotlivých skúšok.

Platnosť a primeranosť skúšobných otázok orgán posudzovania zhody hodnotí najmenej jedenkrát za dva roky.

Okruhy skúšobných otázok musia obsahovať otázky z nasledujúcich odborných domén:

a) Riadenie kybernetickej a informačnej bezpečnosti
b) Riadenie IT služieb
c) Riadenie prístupov
d) IT architektúra
e) Riadenie aktív, hrozieb a rizík
f) Akvizícia, vývoj, implementácia a údržba systémov (SDLC)
g) Riadenie tretích strán a dodávateľských služieb
h) Bezpečnosť prevádzky IT
i) Bezpečnosť počítačových sietí
j) Riešenie incidentov
k) Manažment bezpečnostných zraniteľností
l) Základy bezpečnosti OT/ICS
m) Personálna bezpečnosť
n) Riadenie kontinuity
o) Strategický manažment
p) Legislatíva a štandardy

### 4.3.3 Príprava otázok na odbornú skúšku

Za prípravu otázok pre odbornú skúšku manažéra kybernetickej bezpečnosti je zodpovedný orgán posudzovania zhody.

Množina skúšobných otázok musí byť najmenej 14 dní pred konaním prvej skúšky predložená vlastníkovi certifikačnej schémy na schválenie. Vlastník certifikačnej schémy má výhradné právo na zmenu, pridanie, alebo

odstránenie akejkoľvek otázky z množiny navrhnutých skúšobných otázok. Vlastník certifikačnej schémy sa ku predloženým otázkam vyjadrí najneskôr v lehote do 10 dní. Po schválení množiny otázok vlastníkom schémy, môže orgán posudzovania zhody danú množinu otázok používať v procese skúšky. Orgán posudzovania zhody zabezpečí, aby sa neplatné verzie množín otázok uchovávali v archíve po dobu 3 rokov.

#### 4.3.4 Kvalifikačné požiadavky na skúšajúcich

- Skúšajúci musí spĺňať nasledovné kvalifikačné predpoklady:
- schopnosť plynulo a zrozumiteľne komunikovať v slovenskom alebo českom jazyku,
- ovládanie procesov skúšky, jej priebehu a vyhodnotenia,
- ovládanie technických testovacích prostriedkov (pre dištančnú / online formu skúšky),
- znalosť problematiky, ktorá je predmetom skúšky,
- spoľahlivosť, bezúhonnosť, nestrannosť.

#### 4.3.5 Termín a miesto vykonania odbornej skúšky

Termín a miesto a metódu vykonania odbornej skúšky určuje orgán posudzovania zhody.

Pozvánka na odbornú skúšku sa doručuje žiadateľovi spravidla v elektronickej podobe 15 dní pred termínom konania skúšky.

Ak sa žiadateľ na skúšku nedostaví, ale vopred sa ospravedlní, je automaticky zaradený a pozvaný na najbližší termín.

V prípade, že sa žiadateľ nedostaví ani na náhradný termín odbornej skúšky, orgán posudzovania zhody môže navrhnúť vyradenie tohto žiadateľa zo zoznamu žiadateľov. Vyradenia žiadateľa podlieha schváleniu vedúcim certifikačného orgánu.

Ak kandidát nebol na skúške úspešný, môže sa po obdržaní takéhoto rozhodnutia o skúške prihlásiť na ďalší termín skúšky. Početnosť opakovaní skúšky nie je limitovaná.

#### 4.3.6 Priebeh odbornej skúšky

Test sa vykonáva písomnou formou, a to buď prezenčne alebo dištančne za použitia vhodných technických prostriedkov. O spôsobe vykonania testu musia byť kandidáti informovaní v pozvánke na skúšku.

Priebeh odbornej skúšky riadi vedúci skúšania podľa postupu Pokyny pre skúšajúcich a metodika skúšky, ktoré obsahujú aj postup na vyhodnotenie skúšky.

Pred začatím odbornej skúšky žiadateľ preukáže svoju totožnosť dokladom totožnosti a orgán posudzovania zhody ho poučí o pravidlách priebehu skúšky. Ak žiadateľ pred začatím odbornej skúšky nepreukáže svoju totožnosť alebo sa počas skúšky správa v rozpore s pravidlami priebehu skúšky a dobrými mravmi, vylúči sa zo skúšky a hľadí sa na neho akoby skúšku vykonal neúspešne.

Žiadateľ je po celý čas prípravy a priebehu odbornej skúšky, ktorá sa vykonáva dištančnou formou, monitorovaný použitím video konferenčných nástrojov. V prípade pokynu vedúceho skúšania je žiadateľ povinný preukázať, že v miestnosti sa nenachádza iná osoba.

#### 4.3.7 Vyhodnotenie odbornej skúšky

Skúšajúci vyhodnotí správnosť/nesprávnosť odpovedí. V prípade písomne vykonávanej skúšky prostredníctvom pripravenej šablóny správnych odpovedí. Správne odpovede vyznačí zakrúžkovaním čísla otázky.

V prípade skúšky vykonanej dištančne za použitia technických prostriedkov sú odpovede vyhodnotené pomocou reportovacej funkcie softvérového testovacieho nástroja.

Skúška sa považuje za **úspešnú**, ak kandidát dosiahne **najmenej 70%** správnych odpovedí.

Skúška sa považuje za **neúspešnú** ak kandidát dosiahne v hodnotení **menej ako 70%** správnych odpovedí.

Dokumentácia priebehu a výsledkov odbornej skúšky, testovacie otázky, vyhodnotenia testov a štatistiky úspešnosti nie sú kandidátom sprístupňované.

Sťažnosti na priebeh skúšky alebo vyhodnotenie skúšky, vrátane odvolaní proti vyhodnoteným výsledkom sa vybavujú v zmysle postupu uvedeného v kapitole 6.

# 5 CERTIFIKÁT

## 5.1 ROZHODNUTIE O UDELENÍ CERTIFIKÁTU

Podkladom na vydanie alebo nevydanie certifikátu manažéra kybernetickej bezpečnosti sú **informácie o žiadateľovi a výsledky odbornej skúšky**. Rozhodovanie o tom je nezávislé a nestranné a prijíma ho kompetentná osoba v súlade s požiadavkami na orgán posudzovania zhody podľa technickej normy[4)] a v súlade s touto certifikačnou schémou.

Platnosť certifikátu manažéra kybernetickej bezpečnosti sa začína dňom vydania certifikátu manažéra, ktorý je totožný s dňom rozhodnutia o udelení certifikátu. Certifikát manažéra kybernetickej bezpečnosti sa zasiela žiadateľovi elektronicky a poštou, alebo si ho môže na základe vlastnej žiadosti prevziať osobne.

Doba platnosti certifikátu je **3 roky od jeho vydania**. Manažér kybernetickej bezpečnosti počas doby platnosti certifikátu manažéra kybernetickej bezpečnosti využíva svoj certifikát manažéra v súlade s podmienkami a obmedzeniami v ňom uvedenými poskytuje na vyžiadanie súčinnosť orgánu posudzovania zhody a zaväzuje sa poskytnúť mu pravdivé informácie a dokumenty vyžadované touto schémou. Svoju činnosť vykonáva manažér kybernetickej bezpečnosti odborne a v súlade s dobrými mravmi.

## 5.2 DOHĽAD NAD ČINNOSŤOU CERTIFIKOVANÉHO MANAŽÉRA

V súlade s požiadavkami zákona č. 56/2018 Z.z. o posudzovaní zhody výrobku, sprístupňovaní určeného výrobku na trhu a požiadavkami ISO/IEC 17024:2012 Posudzovanie zhody - Všeobecné požiadavky na orgány vykonávajúce certifikáciu osôb sa posudzovanie zhody môže skončiť udelením atestácie, vo forme certifikátu manažéra kybernetickej bezpečnosti. V niektorých prípadoch sa však z dôvodov udržania platnosti stanoviska vyjadreného atestáciou môže vyžadovať opakovanie funkcií atestácie. Opakovanie funkcie atestácie sa vykonáva formou mimoriadneho dohľadu, t.j. systematického opakovania činností posudzovania zhody ako základu udržania platnosti stanoviska o zhode.

O vykonaní mimoriadneho dohľadu nad činnosťami vykonávanými certifikovanými manažérmi kybernetickej bezpečnosti rozhodne vedenie orgánu posudzovania zhody. Rozhodnutie môže byť vykonané na základe:

- vlastného rozhodnutia, v prípade, že sa podmienky posúdenia objektu posudzovania zhody časom zmenili, čo by mohlo ovplyvniť pokračujúce plnenie požiadaviek na zhodu,
- žiadosti objektu posudzovania zhody, ktorý si vyžaduje ďalšie preukázanie, že požiadavky sa skutočne plnia,
- obdržanej sťažnosti na činnosť manažéra kybernetickej bezpečnosti, alebo na základe informácie o možnom porušovaní povinností podľa tejto certifikačnej schémy.

Činnosti vykonávané pri dohľade sa plánujú s cieľom zabezpečiť potrebu udržať platnosť existujúceho stanoviska vydaného pri rozhodnutí o udelení certifikátu.

V rámci dohľadu sa môže vykonať:

- pohovor s manažérom kybernetickej bezpečnosti s cieľom zistiť jeho znalosti a zručnosti, zvyšovanie znalostí absolvovaním kurzov a pod.,
- kontrola záznamov manažéra kybernetickej bezpečnosti o sťažnostiach zainteresovaných strán, sťažnostiach Národného bezpečnostného úradu, ich vybavenie, nápravné opatrenia a ich účinnosť.

Ak je to potrebné, môže sa pri dohľade vykonať posúdenie vlastného výkonu riadenia kybernetickej bezpečnosti. Na tento účel orgán posudzovania zhody využíva len vlastných zamestnancov. O vykonanom dohľade spracuje orgán posudzovania zhody zápis, ktorý okrem zistených skutočností obsahuje aj termín predloženia nápravných opatrení na odstránenie zistených nedostatkov.

4 ISO/IEC 17024

Zápis orgán posudzovania zhody prerokuje s certifikovaným manažérom kybernetickej bezpečnosti, ktorý svojim podpisom potvrdí oboznámenie sa s protokolom, a ak s niektorými závermi nesúhlasí, uvedie svoje stanovisko (námietky, zdôvodnenie nesúhlasu).

## 5.3 OBNOVA CERTIFIKÁTU A PREDĹŽENIE PLATNOSTI CERTIFIKÁTU

### 5.3.1 Obnova platnosti certifikátu manažéra

O obnovu certifikátu manažéra kybernetickej bezpečnosti možno požiadať aj pred uplynutím doby platnosti aktuálne platného certifikátu manažéra:

a) ak to vyplýva zo všeobecne záväzných právnych predpisov,
b) na základe zmeny požiadaviek certifikačnej schémy,
c) vzhľadom na povahu a zmeny v priemysle alebo odvetví, v ktorom manažér pôsobí,
d) vzhľadom na prebiehajúce zmeny v technológiách a požiadavkách na manažérov alebo
e) na základe odôvodnenej požiadavky zainteresovaných strán.

Na žiadosť, konanie a na vydanie certifikátu manažéra kybernetickej bezpečnosti a na certifikát manažéra kybernetickej bezpečnosti sa vzťahujú ustanovenia o certifikácii manažéra kybernetickej bezpečnosti a certifikačná schéma.

### 5.3.2 Predĺženie platnosti certifikátu manažéra

Pred uplynutím doby platnosti certifikátu manažéra kybernetickej bezpečnosti môže manažér kybernetickej bezpečnosti požiadať o predĺženie platnosti svojho certifikátu manažéra na ďalšie trojročné obdobie. Žiadosť sa podáva najneskôr tri mesiace pred skončením platnosti certifikátu manažéra kybernetickej bezpečnosti.

Podmienkou pre vydanie nového certifikátu manažéra kybernetickej bezpečnosti je, že manažér kybernetickej bezpečnosti:

a) počas doby platnosti certifikátu spĺňa podmienky certifikácie a
b) preukáže, že:
   - si udržiava vedomosti a prax (udržiavanie praktických zručností doložením výkonu praxe manažéra kybernetickej bezpečnosti počas doby platnosti certifikátu),
   - si zvyšuje kvalifikáciu v oblasti kybernetickej bezpečnosti najmenej v rozsahu absolvovania 120 hodín odborného vzdelávania v informačnej a kybernetickej bezpečnosti počas doby platnosti certifikátu,
   - je nezávislý a predchádza konfliktu záujmov (dokladá sa prehlásením) a
   - dokladá nadobudnuté znalosti v oblasti kybernetickej bezpečnosti (dokladá sa praxou, vzdelávaním).

Zvyšovanie kvalifikácie pozostáva najmä z:

- účasti na školeniach, konferenciách a webinároch v oblasti kybernetickej bezpečnosti (doložením rozsahu podujatia v hodinách),
- samoštúdiom odbornej literatúry v rozsahu max. 20 hodín ročne (dokladuje sa čestným prehlásením a zoznamom odbornej literatúry),
- publikačnej činnosti (každá normostrana publikácie sa akceptuje ako jedna hodina),
- prednáškovej činnosti (započítava sa každá odprednášaná hodina, na prípravu prednášky je možné započítať trojnásobok času prednášky pri jedinečnom obsahu prednášky a jedennásobok času prednášania pri opakovanom prednášaní prednášky).

### 5.3.3 Zmena predmetu certifikácie

Certifikačná schéma v tejto verzii nepredpokladá zavedenie rôznych úrovní certifikácie, ani zmenu predmetu certifikácie.

## 5.4 POZASTAVENIE ALEBO ZRUŠENIE CERTIFIKÁTU MANAŽÉRA

Pozastavenie platnosti certifikátu manažéra môže nastať rozhodnutím orgánu posudzovania zhody, alebo na základe požiadania manažéra kybernetickej bezpečnosti.

Pozastavenie alebo zrušenie certifikátu manažéra kybernetickej bezpečnosti orgán posudzovania zhody zváži v nasledujúcich prípadoch:

- Certifikovaná osoba nedodržiava, alebo naďalej už neplní kritériá certifikácie,
- Certifikovanej osobe je dokázané neodborné konanie v oblasti certifikácie,
- Certifikovaná osoba nedodržiava etický kódex,
- Certifikovaný manažér kybernetickej bezpečnosti dobrovoľne požiada o pozastavenie platnosti certifikátu.

Orgán posudzovania zhody je povinný tieto okolnosti prešetriť a prijať príslušné opatrenia. Ak nedôjde v lehote určenej orgánom posudzovania zhody k náprave skutočností, ktoré viedli k pozastaveniu platnosti certifikátu manažéra kybernetickej bezpečnosti, orgán posudzovania zhody ukončí platnosť vydaného certifikátu manažéra kybernetickej bezpečnosti.

Certifikačný orgán vymedzí a oznámi postup pozastavenia a zrušenia certifikátu manažéra kybernetickej bezpečnosti.

### 5.4.1 Pozastavenie platnosti certifikátu na základe podnetu NBÚ

Orgán posudzovania zhody pozastaví platnosť certifikátu manažéra kybernetickej bezpečnosti na základe podnetu Národného bezpečnostného úradu pri porušovaní povinností podľa tejto certifikačnej schémy, najmä:

- Certifikovanej osobe je dokázané neodborné konanie v oblasti certifikácie
- Certifikovaná osoba nedodržiava etický kódex

Platnosť certifikátu môže byť rozhodnutím orgánu posudzovania zhody pozastavená **na dobu najviac 90 dní**. Orgán posudzovania zhody bezodkladne písomne vyzve manažéra kybernetickej bezpečnosti k náprave skutočností, ktoré viedli k pozastaveniu platnosti certifikátu manažéra kybernetickej bezpečnosti.

Ak nedôjde v lehote určenej orgánom posudzovania zhody k náprave skutočností, ktoré viedli k pozastaveniu platnosti certifikátu manažéra, orgán posudzovania zhody ukončí platnosť vydaného certifikátu manažéra kybernetickej bezpečnosti.

### 5.4.2 Pozastavenie platnosti certifikátu na základe požiadavky zainteresovaných strán

Orgán posudzovania zhody pozastaví platnosť certifikátu manažéra kybernetickej bezpečnosti na základe zdôvodnenej písomnej požiadavky niektorej zo zainteresovaných strán. Takéto pozastavenie platnosti certifikátu manažéra kybernetickej bezpečnosti je možné len na dobu určitú, **maximálne však na 1 rok**, z nasledujúcich dôvodov:

- dlhodobej neprítomnosti,
- zo zdravotných dôvodov, alebo
- z dôvodov hroziaceho konfliktu záujmov.

Ak bola platnosť certifikátu pozastavená na základe žiadosti manažéra kybernetickej bezpečnosti po uplynutí doby definovanej manažérom kybernetickej bezpečnosti orgán posudzovania zhody obnoví platnosť vydaného certifikátu manažéra kybernetickej bezpečnosti.

### 5.4.3 Ukončenie platnosti certifikátu

Orgán posudzovania zhody môže ukončiť platnosť vydaného certifikátu manažéra kybernetickej bezpečnosti na základe:

- písomnej požiadavky manažéra kybernetickej bezpečnosti,
- nesplnenia požiadavky na nápravu skutočností, ktoré viedli k pozastaveniu platnosti certifikátu manažéra kybernetickej bezpečnosti v určenej lehote.

Orgán posudzovania zhody uzatvorí s manažérom kybernetickej bezpečnosti dohodu o zdržaní sa používania všetkých odkazov na certifikovaný status manažéra kybernetickej bezpečnosti, ak sa zruší platnosť certifikátu manažéra kybernetickej bezpečnosti.

# 6 VYBAVOVANIE SŤAŽNOSTÍ

Sťažnosti na priebeh skúšky alebo vyhodnotenie skúšky, vrátane odvolaní proti vyhodnoteným výsledkom a sťažnosti na výkon činnosti manažéra kybernetickej bezpečnosti spracúva a rieši orgán posudzovania zhody podľa technickej normy[5] a v zmysle platnej politiky.

Orgán posudzovania zhody je povinný na svojom webovom sídle zverejniť záväznú politiku, ktorou:

- špecifikuje postupy pre vybavovanie sťažností a odvolaní v rámci procesov certifikácie,
- špecifikuje postupy pre vybavovanie sťažností na výkon činností manažéra,
- stanovuje zodpovednosti a zásady riešenia sporov.

# 7 VEDENIE EVIDENCIÍ

Orgán posudzovania zhody vedie evidenciu:

a) žiadostí o vydanie certifikátu manažéra kybernetickej bezpečnosti,
b) dokumentácie priebehu a výsledkov odbornej skúšky,
c) dokladov preukazujúcich splnenie podmienok podľa certifikačnej schémy,
d) vydaných certifikátov manažéra kybernetickej bezpečnosti,
e) iných súvisiacich dokumentov.

# 8 PRÍSTUP K CERTIFIKAČNEJ SCHÉME

Certifikačná schéma je verejný dokument, ktorý zverejňuje Národný bezpečnostný úrad na svojom webovom sídle. Akúkoľvek zmenu certifikačnej schémy, jej aktualizáciu, resp. nové vydanie, musí vlastník certifikačnej schémy preukázateľne zvýrazniť na svojom webovom sídle informáciou o zmene, zverejnením aktualizovanej certifikačnej schémy, ako aj základným popisom príslušnej zmeny. Účinnosť danej zmeny je daná jednoznačnou informáciou uvedenom v texte, ktorý popisuje zmenu na webovom sídle vlastníka schémy a uvedeným dátumom účinnosti v samotnom texte aktualizovanej certifikačnej schémy. Prechodné obdobie medzi vydaním a účinnosťou novej certifikačnej schémy určuje vlastník certifikačnej schémy a to na základe posúdenia charakteru a náročnosti zmien.

V prípade pokrytia tejto certifikačnej schémy manažéra kybernetickej bezpečnosti akreditáciou SNAS, vlastník certifikačnej schémy je povinný informovať SNAS o zmenách certifikačnej schémy.

Dokumenty preukazujúce akreditáciu, resp. dokumenty súvisiace s certifikačným procesom (napr. akreditáciu, záväzné politiky, vzory zmlúv, atď.) zverejňuje orgán posudzovania zhody na svojom webom sídle, v nadväznosti na zmeny certifikačnej schémy.

[5] ISO/IEC 17024

# Etický kódex manažéra kybernetickej bezpečnosti

## Úvod

- Tento etický kódex je určený na podporu etického a profesionálneho správania vo všetkých oblastiach riadenia kybernetickej bezpečnosti. I keď znenie kódexu nie je odvodené od konkrétneho systému manažérstva, témy, ktoré obsahuje, sa týkajú najmä oblasti odbornej činnosti pracovnej roly manažéra kybernetickej bezpečnosti.
- Etický kódex má byť uplatniteľný pre rolu manažéra kybernetickej bezpečnosti všeobecne, v širokom spektre odvetví a typov organizácií.
- V nasledujúcom texte kódexu je podľa pravidiel slovenského pravopisu na spoločné označenie mužských aj ženských reprezentantov profesie používané tzv. generické maskulínum, a forma mužského rodu je chápaná ako všeobecná, označujúca reprezentantov oboch pohlaví.

## Profesijná zodpovednosť

- V reakcii na rýchle zmeny právneho, technologického a ekonomického prostredia, naberá v poslednej dobe pri výkone povolania manažéra kybernetickej bezpečnosti jeho ďalšie vzdelávanie na význame. Manažér kybernetickej bezpečnosti využije svoje odborné zručnosti, vedomosti a úsudok za všetkých okolností legálne, čestne a bezúhonne, s cieľom splnenia oprávnených záujmov zainteresovaných strán, ktorými môžu byť zákazníci, zamestnávatelia, alebo zákazníci zamestnávateľa.
- V súlade s náležitým dodržiavaním zákonných ustanovení a zásad výkonu povolania, musí manažér kybernetickej bezpečnosti vždy konať v najlepšom záujme zákazníka, alebo zamestnávateľa. Záujem zákazníka, alebo zamestnávateľa je povinný povýšiť nad vlastné záujmy a nad záujmy ostatných manažérov kybernetickej bezpečnosti.
- Manažér kybernetickej bezpečnosti podnikne všetky kroky na rozvoj vlastnej odbornej spôsobilosti v súlade s aktuálnym vývojom v profesionálnej oblasti.
- Manažér kybernetickej bezpečnosti si uplatní nárok iba na také členstvá a kvalifikácie, ktoré sú v danom čase platné.
- Manažér kybernetickej bezpečnosti sa zaväzuje vykonávať profesijnú činnosť odborne, objektívne, nestranne a v súlade s príslušnými všeobecne záväznými právnymi predpismi Slovenskej republiky, technickými normami a všeobecne uznávanou najlepšou praxou.
- Manažér kybernetickej bezpečnosti musí za každých okolností konať tak, aby zachoval dôstojnosť a dobrú povesť tejto profesie.
- Manažér kybernetickej bezpečnosti nebude vedome vykonávať činnosť, pre ktorú nemá dostatočné zručnosti, vedomosti a zodpovedajúcu právomoc.
- Akákoľvek reklama výkonu činnosti manažéra kybernetickej bezpečnosti musí byť slušná, legálna, čestná a vecná a nesmie byť vykonávaná ako porovnávanie s konkurenčnými činnosťami a službami.

## Zodpovednosť voči klientom, zákazníkom a zamestnávateľom

- Manažér kybernetickej bezpečnosti musí poskytovať zákazníkom, zamestnávateľovi, alebo zákazníkom zamestnávateľa také odborné služby, ktoré sú profesionálne, objektívne, relevantné a včasné, spolu s príslušnými výhradami, alebo upozorneniami.
- Manažér kybernetickej bezpečnosti sa vyhýba takým činnostiam alebo úlohám, ktoré môžu spôsobiť konflikt záujmov pri výkone jeho pracovných zodpovedností.
- Manažér kybernetickej bezpečnosti je povinný zachovať mlčanlivosť vo vzťahu ku všetkým informáciám, získaným a poskytnutým počas profesijnej činností. Povinnosť zachovávať mlčanlivosť nie je časovo obmedzená. Povinnosť mlčanlivosti sa nevzťahuje na také informácie, u ktorých bolo preukázané, že sú alebo

sa stali známymi bez zavinenia manažéra kybernetickej bezpečnosti ani na informácie, ktoré majú zmluvné strany povinnosť zverejniť v zmysle platných a účinných právnych predpisov Slovenskej republiky.

- Manažér kybernetickej bezpečnosti musí dodržiavať všetky potrebné a primerané opatrenia, aby zabránil vyzradeniu, zneužitiu, poškodeniu, zničeniu, strate alebo odcudzeniu, neoprávnenému prístupu, zmene a rozširovaniu informácií, údajov a dokladov, ktoré získal pri výkone činnosti manažéra kybernetickej bezpečnosti.
- Manažér kybernetickej bezpečnosti nesmie zneužívať svoje postavenie, súvisiace s výkonom jeho činnosti pri uskutočňovaní súkromných záujmov vo vlastný prospech alebo v prospech tretích strán.
- Certifikovaný manažér kybernetickej bezpečnosti je povinný bezodkladne oznámiť orgánu posudzovania zhody akékoľvek okolnosti, ktoré môžu mať potenciálne vplyv na jeho spôsobilosť, schopnosť alebo možnosť naďalej plniť certifikačné požiadavky (napr. prekážky v dodržiavaní kvalifikačných predpokladov, prerušenie celoživotného vzdelávania, odobratie alebo skončenie platnosti odborných certifikátov, zdravotné obmedzenia, osobné prekážky a pod.).

## Zodpovednosť voči podriadeným a kolegom

- Manažér kybernetickej bezpečnosti musí zaručiť primeraný dohľad nad osobami, pracujúcimi v rámci jeho riadiacich právomocí alebo pod jeho dozorom a musí ich povzbudzovať v rozvoji ich odborných spôsobilostí.
- Manažér kybernetickej bezpečnosti sa vyhýba neodôvodnenej negatívnej komunikácii alebo publikovaniu neprimeranej kritiky, v súvislosti s odbornou činnosťou iného manažéra kybernetickej bezpečnosti.
- Manažér kybernetickej bezpečnosti nesmie úmyselne dostať kolegu - manažéra kybernetickej bezpečnosti do situácie, v ktorej by mohol nevedomky porušiť niektorú časť tohto etického kódexu.