MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Návrh etických štandardov pre sektor ITVS

Obsah

Obsah 2
1 Správa dokumentu 3
2 Úvod 4
2.1 Definície a skratky 5
3 Východiskový stav – legislatíva a existujúce etické kódexy na úrovni Slovenskej republiky, Európskej únie 7
3.1 Základné východiská, dokumenty a podklady 7
3.1.1 Súvisiace legislatívne úpravy 7
3.1.2 Ďalšie inštitúcie v SR, EÚ, USA a vo Veľkej Británii 8
3.1.3 Etické kódexy vo vybraných inštitúciách vo svete 8
4 Úvod do problematiky etických štandardov v prostredí informačných technológií verejnej správy 10
5 Základné princípy etického správania 11
6 Návrh súboru štandardov ako východisko pre tvorbu etických kódexov 13
6.1 Etické štandardy pre zamestnancov ITVS 13
6.2 Etické štandardy pre certifikovaných bezpečnostných špecialistov 16
6.3 Etické štandardy pri bezpečnostnom monitoringu 16
6.4 Etické štandardy pri riešení kybernetických bezpečnostných incidentov 17
6.5 Etické štandardy pri bezpečnostných testoch alebo penetračnom testovaní 17
6.5.1 Etické kódexy a audítorské štandardy pre penetračné testy v USA a Spojenom kráľovstve 17
6.5.2 Návrh prístupu k etickým štandardom 18
6.5.3 Právne a etické súvislosti pri penetračnom testovaní 19
6.6 Základ pre tvorbu štandardov uplatňovaných pri výbere dodávateľa, služby a technológie. 20
6.7 Základ pre tvorbu štandardov uplatňovaných pri výbere bezpečnostných špecialistov pri prijímaní do zamestnania 21
6.8 Ďalšie doplňujúce ustanovenia 22
7 Usmernenie pri tvorbe etických kódexov v podmienkach OVM 23

1 Správa dokumentu

Tento dokument je metodickým materiálom slúžiacim pre potreby orgánov verejnej moci, ktorý nie je povinný na použitie a ani nie je záväzný. Dokument je poskytnutý voľne a bezplatne na využitie podľa potrieb konkrétnej organizácie.

Vytvorený dokument je možné použiť i pre potreby vzdelávania pracovníkov organizácií v oblasti kybernetickej a informačnej bezpečnosti.

Vytvorený dokument nie je určený na ďalší predaj alebo akúkoľvek inú komerčnú či obchodnú činnosť.

Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (ďalej aj „MIRRI“) nezodpovedá za nesprávne použitie predmetného dokumentu zo strany organizácie. Správne použitie a implementácia bezpečnostných opatrení je plne v kompetencii a zodpovednosti konkrétnej organizácie.

MIRRI si vyhradzuje právo na zmenu/úpravu predmetného dokumentu alebo čiastkových textov a tabuliek, a to v potrebnom rozsahu vrátane zmien verzií dokumentov. Dokument je pilotným výstupom v rámci Reformy Štandardizácia technických a procesných riešení kybernetickej a informačnej bezpečnosti (Plán obnovy a odolnosti).

2 Úvod

Zvyšujúce sa využívanie informačných a komunikačných technológií vo všetkých sférach moderného života na jednej strane robí svet bohatším, efektívnejším a interaktívnejším miestom, na druhej strane to však zvyšuje aj jeho krehkosť, pretože posilňuje našu závislosť od systémov informačných a komunikačných technológií, ktoré nikdy nemôžu byť úplne bezpečné.

Kybernetická bezpečnosť sa preto stala predmetom celosvetového záujmu a významu. V tejto súvislosti môžeme v dnešnom diskurze o kybernetickej bezpečnosti pozorovať takmer neustály dôraz na neustále rastúci a rôznorodý súbor hrozieb, od základných počítačových vírusov až po sofistikované druhy kyberzločinu a kyberšpionážnych aktivít, ako aj kybernetický teror a kybernetickú vojnu.

Táto rastúca zložitosť digitálneho ekosystému v kombinácii s rastúcimi globálnymi rizikami vytvorila nasledujúcu dilemu. Prílišné zdôrazňovanie kybernetickej bezpečnosti môže porušovať základné hodnoty, akými sú rovnosť, spravodlivosť, sloboda alebo súkromie. Zanedbanie kybernetickej bezpečnosti by však mohlo podkopať dôveru občanov v digitálnu infraštruktúru, v tvorcov politík a v štátne orgány.

Kybernetická bezpečnosť teda podporuje ochranu hodnôt, ako je nepoškodzovanie, súkromie a dôvera, a preto medzi hodnotami vytvára zložitý vzťah: niektoré môžu byť podporné a iné protichodné, v závislosti od kontextu. Napríklad, zatiaľ čo kybernetická bezpečnosť je vo väčšine prípadov predpokladom ochrany údajov, a teda súkromia ľudí, môže tiež sprístupniť súkromné informácie odborníkom na kybernetickú bezpečnosť s cieľom odhaliť škodlivé aktivity. (The Ethics of Cybersecurity, 2020, kap. 2.1)

V nadväznosti na vyššie uvedené, je tiež potrebné aj v kyberpriestore dodržiavať určité štandardy etického správania sa a preto je potrebné vypracovať etický kódex ako všeobecné usmernenie, resp. štandard pre štátnu a verejnú správu.

Etický kódex je súbor všeobecne uznávaných a všeobecne uplatňovaných morálnych noriem, ideálov a štandardov spoločnosti, pre ktorú je určený, ktoré idú nad rámec práva a legislatívy. Je jedným z najvýznamnejších spôsobov vnášania etiky do každodenného života a usmerňovania správania sa člena tejto spoločnosti. Mal by vystihovať aj špecifiká jednotlivých spoločností a vychádzať z potrieb spoločnosti, pre ktorú bol ustanovený.

Etický kódex by mal byť verejne prístupný, zrozumiteľný, jednoznačný a kontrolovateľný verejnosťou.

Etický kódex uľahčuje rozhodovanie človeka o tom, čo je správne a nesprávne, v pre neho nejasných situáciách. Pomáha predchádzať konfliktom, pomáha upraviť správanie jednotlivcov či skupín v súlade so záujmom spoločnosti, bezpečnostných pracovníkov v oblasti kybernetickej bezpečnosti nevynímajúc.
V nadväznosti na vyššie uvedené, budovanie etických štandardov by malo plniť nasledujúce ciele:

- výchovno-vzdelávaciu – budovať povedomie o týchto otázkach a budovať povedomie snahy o etickosť vo verejnej správe,
- informatívnu vo vzťahu k zamestnancom verejnej správy – informovať zamestnancov vo verejnej správe, akého konania by sa mali zdržať, aby si boli vedomí, že konajú nesprávne, resp. protizákonne,
- preventívnu – na jeho základe zabraňovať, aby pri činnosti zamestnancov vo verejnej správe nastávalo porušenie zákonov,
- penalizačnú – umožniť a zakotviť účinnú reakciu na porušenie etického kódexu,

- facilitatívnu – systematizovať a uľahčovať odhalenie konfliktu záujmov zamestnancov vo verejnej správe.

2.1 Definície a skratky

Pojem	Vysvetlenie
Bezpečnostný tím	Skupina zamestnancov zastávajúcich niektorú z bezpečnostných rolí
Dominantné postavenie na trhu	na relevantnom trhu má podnikateľ alebo niekoľko podnikateľov, ktorí nie sú vystavení podstatnej súťaži a ktorí sa vzhľadom na svoju ekonomickú silu môžu správať nezávisle. Dominancia bola definovaná európskym súťažným právom ako pozícia ekonomickej sily podnikateľa, ktorá mu umožňuje brániť udržiavaniu efektívnej súťaže na relevantnom trhu tým, že sa môže správať v značnom rozsahu nezávisle od svojich konkurentov, zákazníkov a v konečnom dôsledku aj spotrebiteľov. Schopnosť správať sa nezávisle sa pritom odvíja od stupňa súťažných tlakov, ktoré sú na neho vyvíjané. Dominancia je stav, keď súťažné tlaky vyvíjané na podnikateľa nie sú dostatočné a tak môže mať podnikateľ v dominantnom postavení podstatnú trhovú silu počas dlhšej doby. Vo všeobecnosti je dominancia určovaná viacerými faktormi, ktoré posudzované samostatne nemusia byť určujúce (zdroj: https://www.antimon.gov.sk/-8-zneuzivanie-dominantneho-postavenia/).
Hospodárska súťaž	súperenie medzi podnikmi v boji o zákazníka. Je to jeden zo základných mechanizmov trhovej ekonomiky. Hospodárska súťaž umožňuje súťažiteľom slobodne rozvíjať svoju súťažnú činnosť v záujme dosiahnutia hospodárskeho prospechu a vytvára podmienky združovať sa na výkon tejto činnosti.
Konflikt záujmov	predstavuje ohrozenie princípu objektívnosti a nezaujatosti, ktorý vzniká, ak zamestnanec vykonáva odbornú činnosť pre dve alebo viac strán, ktorých záujmy sú v konflikte, prípadne ak záujem zamestnanca je v konflikte so záujmom strany, ktorú zastupuje.
Need to know	„potrebuje vedieť“ – požiadavka, aby sa s daným okruhom informácií zoznamoval len nevyhnutne potrebný okruh a počet osôb, tzn. určia sa len tie osoby, ktorým nutnosť zoznamovania sa s danými informáciami vyplýva z plnenia ich služobných/pracovných povinností.
Zamestnanec	Zamestnanec / pracovník štátnej správy alebo verejnej správy alebo zamestnanec pracujúci na dohodu

Skratka	Vysvetlenie
CISA	Certified Information Systems Auditor®
CISM	Certified Information Security Manager®
DDoS	Distributed Denial of Service (distribuované odoprenie služby – typ kybernetického útoku)
DoS	Denial of Service (odoprenie služby – typ kybernetického útoku)
ES	Európska smernica
EÚ	Európska únia
IKT	informačné a komunikačné technológie

Skratka	Vysvetlenie
IS	informačný systém
ISACA	Information Systems Audit and Control Association
IT	informačné technológie
ITVS	Informačné technológie verejnej správy
KB	kybernetická bezpečnosť
KIB	kybernetická a informačná bezpečnosť
MIRRI	Ministerstvo investícií, regionálneho rozvoja a informatizácie SR
MKIB	manažér kybernetickej a informačnej bezpečnosti
NBÚ	Národný bezpečnostný úrad
OVM	orgány verejnej moci
OvZP	organizácie v zriaďovateľskej pôsobnosti
SR	Slovenská republika
VS	verejná správa
Vyhláška č. 179/2020 Z. z.	Vyhláška č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy
Vyhláška č. 400/2019 Z. z.	Vyhláška č. 400/2019 Z. z., ktorou sa vydáva Etický kódex štátneho zamestnanca
Zákon o štátnej službe	Zákon č. 55/2017 Z. z. o štátnej službe a o zmene a doplnení niektorých zákonov
Zákon o výkone práce vo verejnom záujme	Zákon č. 552/2003 Z. z. o výkone práce vo verejnom záujme
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

Pozn.:
Verejná správa na Slovensku zahŕňa:

- Ústrednú a miestnu (všeobecnú a špecializovanú) štátnu správu,
- Územnú a záujmovú samosprávu,
- a ostatnú verejnú správu.

V nadväznosti na uvedené a na účely vypracovania tohto dokumentu, bude v celom texte pod pojmom verejná správa chápaná primárne celá štátna správa a územná samospráva.

3 Východiskový stav – legislatíva a existujúce etické kódexy na úrovni Slovenskej republiky, Európskej únie

Východiskový stav určujú najmä súvisiace legislatívne úpravy predovšetkým Etický kódex štátneho zamestnanca (Vyhláška č. 400/2019 Z. z., ktorou sa vydáva Etický kódex štátneho zamestnanca), ale z pohľadu kybernetickej a informačnej bezpečnosti (ďalej len „KIB“) tiež Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „ZoKB“) a Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov (ďalej len „ZoITVS“). Ďalej sú to inštitúcie v SR (ÚV SR), v EÚ (Rada Európy). Do úvahy je možné vziať aj etické kódexy štátnych zamestnancov, napríklad Veľkej Británie, USA alebo iných krajín (viď. podkapitola 2.1). Špecifiká etiky v kybernetickej bezpečnosti popisuje napríklad kniha „The Ethics of Cybersecurity“ (portál Springer, dostupná na: https://link.springer.com/book/10.1007/978-3-030-29053-5).

V prípade kategórií bezpečnostných špecialistov, ako manažér kybernetickej a informačnej bezpečnosti (ďalej len „MKIB“), alebo audítor kybernetickej bezpečnosti, penetračný tester, špecialista pre riešenie alebo vyšetrovanie kybernetických incidentov, je potrebné uviesť, že títo sú rovnako zaviazaní dodržiavaním etických kódexov, ktorými ich zaviazali certifikačné orgány, resp. organizácie, ktoré im certifikáty vydávali a taktiež ich udržiavajú. Dodržiavanie týchto etických kódexov je teda nevyhnutné na udržanie si pridelených certifikátov. V prípade audítora kybernetickej bezpečnosti a MKIB sú to všetky aktuálne (toho času existujúce) a v budúcnosti existujúce certifikačné orgány.

3.1 Základné východiská, dokumenty a podklady

3.1.1 Súvisiace legislatívne úpravy

Pri vypracovaní tohoto metodického materiálu sa vychádza predovšetkým z/zo:

- Zákona č. 55/2017 Z. z. o štátnej službe a o zmene a doplnení niektorých zákonov,
- Zákona č. 552/2003 Z. z. o výkone práce vo verejnom záujme,
- Zákona č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov,
- Vyhlášky Úradu vlády Slovenskej republiky č. 400/2019, ktorou sa vydáva Etický kódex štátneho zamestnanca,
- Zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- Vyhlášky Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 85/2020 Z. z. o riadení projektov,
- Vyhlášky Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy,
- Zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a doplnení niektorých zákonov v znení neskorších predpisov,
- Vyhlášky Národného bezpečnostného úradu č. 165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov,

- 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,
- Vyhlášky Národného bezpečnostného úradu č. 492/2022 Z. z., ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti,
- Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (Smernica NIS) – v kontexte jej transpozície do právneho poriadku Slovenskej republiky,
- Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 o opatreniach na dosiahnutie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (Smernica NIS2) – v kontexte jej transpozície do právneho poriadku Slovenskej republiky (nahrádza smernicu NIS).

3.1.2 Ďalšie inštitúcie v SR, EÚ, USA a vo Veľkej Británii

- Rada pre štátnu službu (https://radaprestatnusluzbu.vlada.gov.sk/eticky-kodex-statneho-zamestnanca/),
- Rada Európy – Odporúčanie Výboru ministrov Rady Európy č. R (2000) 10 členským štátom o etickom kódexe verejných činiteľov (https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805e2e52),
- USA - Štandardy etického správania (Standards of Ethical Conduct for Employees of the Executive Branch) (Office of Government Ethics) (https://www.oge.gov/web/oge.nsf/resources_standards-of-conduct),
- Veľká Británia - Kódex štátneho zamestnanca (The Civil Service Code) (https://www.gov.uk/government/publications/civil-service-code/the-civil-service-code),
- The Ethics of Cybersecurity (voľne dostupná kniha na portáli Springer) (https://link.springer.com/book/10.1007/978-3-030-29053-5).

3.1.3 Etické kódexy vo vybraných inštitúciách vo svete

- Commitee on Professional Ethics (ACM code of ethics and professional conduct), dostupné na: https://ethics.acm.org/,
- Harvard university - IT Professional Code of Conduct to Protect Electronic Information, dostupné na: https://huit.harvard.edu/files/huit20/files/it_professional_code_of_conduct.pdf,
- UK CyberSecurity Council – Code of ethics form member organisations, dostupné na: https://www.ukcybersecuritycouncil.org.uk/media/0f1emde3/code-of-ethics-july-2021.pdf,
- IEEE code of ethics, dostupné na: https://www.ieee.org/about/corporate/governance/p7-8.html,
- CSIRT Code of Practice, dostupné na: https://www.trusted-introducer.org/TI-CCoP.pdf,
- Forum of Incident Response and Security Teams (FIRST) Ethics for Inceident Response and Security Teams, dostupné na: https://www.first.org/global/sigs/ethics/ethics-first-20191202.pdf,
- A Code of Conduct for Computer Forensic Investigators, dostupné na: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=10165cbe1059143cb41988be1aeec68daccd5351,

- Code of Ethics and Conduct, dostupné na: http://www.corcosconsulting.com/blog/wp-content/uploads/2016/06/Code-of-Ethics-and-Conduct-CyberSecurity-Institute.pdf.

4 Úvod do problematiky etických štandardov v prostredí informačných technológií verejnej správy

Základné etické štandardy v prostredí informačných technológií verejnej správy (ďalej len „ITVS“) je vhodné definovať rovnako, ako všeobecné štandardy, ktoré sú platné pre zamestnancov štátnej správy, verejnej správy, ako aj ďalších zamestnancov v zamestnaneckom pomere na dohodu alebo obdobnom pracovnoprávnom vzťahu. Preto je vhodné vychádzať z princípov definovaných Vyhláškou č. 400/2019 Z. z. platnou pre štátnu správu, ktoré je ďalej možné rozšíriť aj na inú verejnú správu a orgány verejnej moci (ďalej len „OVM“).

Tieto etické štandardy sa v tomto dokumente budú uvažovať v kontexte kybernetickej bezpečnosti v prostredí ITVS.

Ako bolo uvedené vyššie, etické správanie zamestnanca je správanie založené na morálnych hodnotách, ktoré sú postavené na princípoch etiky, teda tých, ktoré idú nad rámec práva.

Pri etických štandardoch v prostredí ITVS sa myslí na kontext informačných systémov verejnej správy, čiže administrácie informačných systémov a kybernetickej bezpečnosti, pri výkone ktorých platí nasledujúce:

- Zamestnanec si uvedomuje vážnosť služby v prostredí ITVS a je zodpovedný za dodržiavanie štandardov etického správania.
- Organizácia rozvíja a podporuje etické správanie zamestnancov a zapracúva uplatňovanie etického kódexu do všetkých oblastí riadenia zamestnancov verejnej správy, teda aj do oblasti riadenia kybernetickej bezpečnosti.
- Nadriadený vedie podriadených zamestnancov k dodržiavaniu etického kódexu najmä prostredníctvom osobného príkladu, zabezpečením oboznámenia sa zamestnancov s jeho obsahom a vyžadovaním a podporovaním etického správania zamestnancov.
- Zamestnanec sa môže obrátiť na priameho nadriadeného vedúceho zamestnanca, ak má pochybnosti o tom, či je jeho správanie v súlade s požiadavkami etického kódexu.
- Zamestnanec, ktorý má podozrenie o porušení etického kódexu, môže písomne oznámiť túto skutočnosť vedúcemu zamestnancovi (priamo nadriadenému vedúcemu zamestnancovi).
- Zamestnanec, ktorý oznámi podozrenie o porušení etického kódexu alebo poukáže na neetické konanie, nemôže byť pre túto skutočnosť žiadnym spôsobom znevýhodňovaný alebo postihovaný.

Tieto východiská sú rozpracované do štandardov v kontexte ITVS v kapitolách nižšie.

5 Základné princípy etického správania

V prostredí ITVS je možné považovať nasledujúce princípy etického správania sa za základ, od ktorého sa odvíja jednak budovanie etických štandardov a následne tvorba samotného etického kódexu v špecifických podmienkach OVM.

Politická neutralita
Zamestnanec pri výkone zamestnania v oblasti kybernetickej bezpečnosti vo verejnej správe dodržiava etický kódex tak, že nevzbudzuje pochybnosť o tom, že koná výlučne vo verejnom záujme.

Nestrannosť
Zamestnanec pri výkone pracovných a služobných povinností dodržiava kódex tak, že koná a rozhoduje vždy objektívne, nestranne, bez predsudkov a zaujatosti. Zohľadňuje práva, povinnosti a právom chránené záujmy všetkých dotknutých strán. Koná a rozhoduje na základe riadne zisteného skutkového stavu veci, pričom dbá na rovnosť dotknutých strán tak, že nedochádza k ujme na ich právach a právom chránených záujmoch. Správa sa tak, že nenarúša dôveru v nestrannosť a objektivitu jeho konania a rozhodovania.

Verejný záujem
Zamestnanec pri výkone štátnej služby a verejnej služby koná výhradne vo verejnom záujme a zdrží sa konania, ktoré by mohlo viesť ku konfliktu verejného záujmu s jeho osobnými záujmami.

Zamestnanec predchádza konfliktu záujmov.

Zamestnanec koná vo verejnom záujme, najmä ak
- sa zdrží osobných záujmov alebo záujmov inej fyzickej osoby alebo právnickej osoby, ktoré môžu ovplyvniť výkon verejnej správy vo verejnom záujme,
- vykoná všetky potrebné úkony na prevenciu a na riešenie konfliktu záujmov,
- nezneužíva informácie získané v súvislosti s vykonávaním svojho zamestnania na osobný záujem alebo záujem inej fyzickej osoby alebo právnickej osoby,
- sa vyhýba nezákonnému zvýhodňovaniu fyzickej osoby a právnickej osoby, ktorá spolupracuje alebo má záujem spolupracovať so štátom,
- neponúka a neposkytuje fyzickej osobe alebo právnickej osobe žiadnu výhodu vyplývajúcu z jeho služobného postavenia,
- prekonzultuje situáciu so svojím nadriadeným pri pochybnostiach, či sú jeho aktivity mimo výkonu štátnej služby alebo verejnej služby zlučiteľné s jeho postavením zamestnanca,
- nezneužíva svoje postavenie alebo funkciu v záležitostiach, ktoré nesúvisia s plnením jeho služobných úloh.

Dôstojnosť a rešpekt v medziľudských vzťahoch
Zamestnanec pri plnení svojich úloh postupuje zdvorilo, s porozumením a ochotou.

Zamestnanec koná s verejnosťou, ostatnými zamestnancami a predstaviteľmi orgánov verejnej moci čestne a v súlade so zásadami slušného správania.

Zamestnanec dbá na dobré medziľudské vzťahy, podporuje spoluprácu a posilňuje vnímanie štátnej služby a verejnej služby ako založenej na pravidlách rovnakého zaobchádzania.

Zamestnanec sa zdrží konania, ktoré poškodzuje zamestnancov upozorňujúcich na všetky formy neetického a protiprávneho konania.

Profesionalita
Zamestnanec dbá na dodržiavanie etického kódexu tak, že plní služobné úlohy svedomito, na vysokej odbornej úrovni, snaží sa o čo najlepšie výsledky a podporuje a presadzuje ustanovenia etického kódexu.

Zamestnanec je zodpovedný za kvalitu vykonávaných služobných úloh a za rozvoj svojich schopností, vedomostí a zručností.

Zamestnanec dbá na to, že verejné zdroje a majetok vo vlastníctve štátu sú využívané hospodárne a účelne, pričom zohľadňuje krátkodobé hľadisko aj dlhodobé hľadisko.

Zamestnanec informácie získané pri vykonávaní štátnej služby a verejnej služby chráni a poskytuje výlučne podľa všeobecne záväzných právnych predpisov, služobných predpisov a ostatných vnútorných predpisov organizácie.

6 Návrh súboru štandardov ako východisko pre tvorbu etických kódexov

Na základe vyššie uvedeného je možné definovať základný súbor štandardov ako východisko pre tvorbu etických kódexov pre nasledujúce špecifické oblasti:

- zamestnanci ITVS,
- certifikovaní bezpečnostní špecialisti,
- riešenie kybernetických bezpečnostných incidentov,
- bezpečnostné testy a penetračné testovanie,
- výber dodávateľa, služby a technológie,
- výber bezpečnostných špecialistov pri prijímaní do zamestnania.

6.1 Etické štandardy pre zamestnancov ITVS

1. Zamestnanec využije svoje odborné zručnosti, vedomosti a úsudok za všetkých okolností legálne, čestne a bezúhonne, s cieľom splnenia oprávnených záujmov zainteresovaných strán, ktorými môžu byť občania, klienti-zákazníci.
2. V súlade s náležitým dodržiavaním zákonných ustanovení a zásad výkonu povolania, musí Zamestnanec vždy konať v najlepšom záujme organizácie. Záujem organizácie je povinný povýšiť nad vlastné záujmy a nad záujmy ostatných zamestnancov alebo nadriadených zamestnancov.
3. Zamestnanec podnikne všetky kroky na rozvoj vlastnej odbornej spôsobilosti v súlade s aktuálnym vývojom v príslušnej profesionálnej oblasti.
4. Zamestnanec si uplatní nárok iba na toho času platné členstvá v organizáciách alebo profesijných združeniach (napr. ISACA) a kvalifikácie (osvedčenia alebo certifikáty súvisiace so zastávanou bezpečnostnou rolou).
5. Zamestnanec 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.
6. Zamestnanec musí za každých okolností konať tak, aby zachoval dôstojnosť a dobrú povesť organizácie.
7. Zamestnanec nebude vedome vykonávať činnosť, pre ktorú nemá dostatočné zručnosti, vedomosti a zodpovedajúcu právomoc.
8. Zamestnanec pri plnení úloh vyplývajúcich z danej bezpečnostnej roly spolupracuje so štátnymi orgánmi a územnou samosprávou v oblasti KIB, ak si to situácia a okolnosti vyžadujú.
9. Zamestnanec musí vyžadovať od dodávateľa také odborné služby, ktoré sú profesionálne, objektívne, relevantné a včasné, spolu s príslušnými výhradami, alebo upozorneniami.
10. Zamestnanec sa vyhýba takým činnostiam alebo úlohám, ktoré môžu spôsobiť konflikt záujmov pri výkone jeho pracovných zodpovedností.
11. Zamestnanec je povinný zachovávať mlčanlivosť vo vzťahu ku všetkým informáciám, získaným a poskytnutým počas profesijnej činnosti. 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 jeho zavinenia, ani na informácie, ktoré majú zmluvné strany povinnosť zverejniť v zmysle platných a účinných právnych predpisov Slovenskej republiky.
12. Zamestnanec 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 pracovnej činnosti alebo v rámci pracovnej náplne.

13. Zamestnanec si uvedomuje, že zlyhanie jednotlivca v oblasti etiky má dopad na verejnú správu ako celok a preto ide ostatným príkladom.
14. Zamestnanec 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.
15. Zamestnanec sa vyhýba neodôvodnenej negatívnej komunikácii alebo publikovaniu neprimeranej kritiky, v súvislosti s odbornou činnosťou iného zamestnanca v sektore ITVS.
16. Zamestnanec nesmie úmyselne dostať kolegu alebo akúkoľvek inú osobu do situácie, v ktorej by mohla nevedomky porušiť niektorú časť etického kódexu.
17. Rešpektovanie štandardov etiky je vecou profesionálnej cti zamestnanca.
18. Zamestnanec bude dodržiavať princípy „need to know“.

Pri používaní pracovnej stanice alebo IS OVM je zamestnanec povinný vykonávať svoju služobnú/pracovnú činnosť v súlade s právnymi predpismi, internými riadiacimi aktami, schválenými etickými štandardami a ďalšími predpismi súvisiacimi s výkonom jeho služobnej/pracovnej činnosti, pričom smerom k ostatným IS OVM alebo IS tretej strany:

a) sa nebude pokúšať prekonávať alebo obchádzať bezpečnostné opatrenia týchto IS,
b) nebude úmyselne vyhľadávať, získavať alebo vykonávať činnosti vedúce k neoprávnenému získaniu alebo zmene prístupových údajov a oprávnení do týchto IS,
c) nebude sa neoprávnene prihlasovať alebo pokúšať sa o prihlásenie sa do týchto IS pomocou neoprávnene získaných prihlasovacích údajov a oprávnení,
d) nebude sa pokúšať pristupovať, modifikovať alebo kopírovať údaje, informácie alebo materiály, ktoré sú blokované, filtrované alebo ak na prístup k nim nebolo používateľovi udelené príslušné oprávnenie,
e) nebude maskovať alebo meniť vlastnú identitu v týchto IS,
f) sa nebude pokúšať vykonávať akýkoľvek monitoring na týchto IS OVM,
g) nebude vykonávať iné činnosti, ktorých následkom bude spôsobená škoda OVM, tretej strane alebo porušené všeobecne záväzné právne predpisy.

Pri používaní služieb elektronickej pošty je zamestnanec povinný najmä:

a) využívať službu elektronickej pošty len na plnenie služobných alebo pracovných povinností,
b) dodržiavať všeobecné morálne a etické štandardy komunikácie (nepoužívať znevažujúce, obscénne, vulgárne, výhražné alebo hrubé vyjadrenia),
c) dbať na to, aby využívaním služby nevystavil riziku infraštruktúru IKT OVM, najmä infiltrácii škodlivým kódom,
d) neprezentovať v emailovej komunikácii svoje osobné názory a postoje ako názory a postoje daného OVM, tieto je možné prezentovať len ak to vyplýva z plnenia služobných alebo pracovných úloh,
e) zabezpečiť pri posielaní citlivých informácií (osobné údaje, obchodné tajomstvo a pod.) jej obsah napríklad použitím šifrovania správy alebo zabezpečením prílohy heslom alebo pripojením prílohy ako zaheslovaného archívu (ZIP, RAR) so zaslaním hesla iným komunikačným kanálom (napr. SMS),
f) zdržať sa zasielania „reťazových“ správ,
g) nefalšovať, nemeniť, alebo nepotláčať identitu odosielateľa správy.

Pri využívaní internetu je zamestnanec povinný najmä:

a) prednostne využívať službu na plnenie služobných alebo pracovných povinností,

b) dodržiavať všeobecné morálne a etické štandardy komunikácie (nepoužívať znevažujúce, obscénne, vulgárne, výhražné alebo hrubé vyjadrenia),
c) dbať na to, aby využívaním služby nevystavil riziku infraštruktúru IKT OVM, najmä infiltrácii škodlivým kódom,
d) nevkladať (do webových stránok, portálov a pod.) svojvoľne príspevky, komentáre týkajúce sa OVM, ktoré neboli vopred schválené komunikačným odborom OVM ,
e) neprezentovať na internete svoje osobné názory a postoje ako názory a postoje daného OVM, tieto je možné prezentovať iba v prípade, ak to vyplýva z plnenia služobných alebo pracovných úloh,
f) neinštalovať softvér dostupný z internetu, ktorý nebol OVM riadne schválený a zakúpený,
g) nesťahovať, nereprodukovať a nedistribuovať neoprávnene softvér, hudbu, fotografie, videá alebo iný materiál, ktorý je chránený autorskými právami,
h) nenavštevovať webové stránky, ktorých charakter je v rozpore so všeobecne záväznými právnymi predpismi (rasistické, podporujúce násilie, schvaľujúce trestnú činnosť, detská pornografia a pod.), neprijímať, nezasielať, nezdieľať sexuálne explicitné materiály alebo materiály, ktorých charakter je v rozpore so všeobecne záväznými právnymi predpismi,
i) nevystavovať interné alebo chránené informácie (ochrana informácií) akýmkoľvek spôsobom na internete,
j) pri využívaní služieb a aplikácií sociálnych sietí je zakázané zverejňovanie alebo vystavovanie súkromných údajov a zverejňovanie alebo vystavovanie súkromných údajov majúcich akýkoľvek súvis so služobnými alebo pracovnými povinnosťami (napr. údaje o zamestnaní, termíny služobných, pracovných ciest alebo lokalít a pod.), povolené je to len ak ide o plnenie služobných alebo pracovných úloh.

Porušenie ustanovení uvedených podľa predchádzajúceho odseku sa považuje za závažný alebo menej závažný bezpečnostný incident (podľa posúdenia konkrétneho prípadu) a môže sa považovať za porušenie pracovnej disciplíny alebo závažné porušenie pracovnej disciplíny. Definovanie a riešenie porušenia pracovnej disciplíny, ako aj z nej vyplývajúce sankcie voči dotknutému zamestnancovi sú v gescii daného OVM.

Vedúci zamestnanci

Vedúci zamestnanci nesmú vyžadovať od podriadených zamestnancov plnenie úloh, ktoré sú v rozpore so všeobecne záväznými predpismi a internými riadiacimi aktmi úradu, nepatria podľa osobitných predpisov do pôsobnosti OVM alebo patria do výlučnej pôsobnosti vedúceho zamestnanca.

Vedúci zamestnanci nesmú zneužívať svoje postavenie voči iným zamestnancom, najmä vynucovaním správania nad rámec ich služobných/pracovných povinností.

Vedúci zamestnanci upevňujú dobré vzťahy medzi zamestnancami, podporujú ich plnenie úloh, spravodlivo ich hodnotia, poskytujú im včas a zrozumiteľne informácie a podklady potrebné na plnenie úloh a bez zbytočného odkladu riešia vzniknuté konflikty.

Vedúci zamestnanci sú zodpovední aj za dodržiavanie etických štandardov na pracovisku, ktoré riadia, zároveň idú príkladom podriadeným zamestnancom.

6.2 Etické štandardy pre certifikovaných bezpečnostných špecialistov

Jednotlivé bezpečnostné roly vo vzťahu k certifikovaným bezpečnostným špecialistom sú definované aktuálne platnou legislatívou a metodickými pokynmi vydanými sektorovým ústredným orgánom pre riadenie KB v sektore VS.

Z bezpečnostného hľadiska majú certifikovaní bezpečnostní špecialisti prístup ku citlivým údajom alebo informáciám, ktoré

- predstavujú popis alebo obsahujú samotné bezpečnostné konfigurácie,
- popisujú usporiadanie bezpečnostných opatrení a spôsoby metódy zabezpečenia IS a sietí,
- predstavujú popis bezpečnostných slabín (napr. zraniteľností) súvisiacich technológií, IS a sietí.

Disponujú informáciami alebo majú prístup ku informáciám, ktoré
- sú obchodným tajomstvom,
- podliehajú autorským právam.

Certifikované osoby, ako certifikovaný audítor kybernetickej bezpečnosti, ako aj MKIB sa primárne riadia etickými kódexmi organizácií, ktoré týchto bezpečnostných expertov certifikujú.

Rovnako ďalší bezpečnostní špecialisti, ktorí sú certifikovaní certifikačnými autoritami alebo certifikačnými organizáciami, sú vždy viazaní etickými pravidlami týchto inštitúcií alebo organizácií. Porušenie etických pravidiel môže viesť k odobratiu certifikátu alebo udelenej licencie.

6.3 Etické štandardy pri bezpečnostnom monitoringu

V prípade bezpečnostného monitoringu je potrebné nahliadať na spôsoby, ako sú dáta zbierané a ukladané z monitoringu sietí, informačných systémov alebo aplikácií. Je potrebné analyzovať, do akej miery sú ich analýzou dotknuté aj etické štandardy. Hranicu medzi oprávneným bezpečnostným monitoringom a už neoprávneným zberom údajov je potrebné určiť a precízne zvážiť vopred (pri nastavovaní monitoringu a zberu dát). V prípade zberu priveľkého množstva informácií, ktoré nie je možné dodatočne obhájiť, sa jedná o možné porušenie legislatívy alebo etických štandardov.

Ďalším dôležitým krokom pri nastavovaní bezpečnostného monitoringu je nastavenie prístupov ku zozbieraným údajom (spravidla tzv. log súborom) alebo ku výstupom zo systémov bezpečnostného monitoringu. Aj v tomto prípade je z pohľadu etických štandardov potrebné použiť princíp need to now (minimálne prístupové práva, len pre exaktne určených bezpečnostných špecialistov, len na obmedzené skupiny relevantných informácií).

Rovnako je potrebné zvažovať prístup zástupcov tretích strán (dodávateľ, servis, externá bezpečnostná služba) ku bezpečnostnému monitoringu a jeho údajom.

Aby bolo možné zamedziť porušovaniu etických štandardov v prípade bezpečnostného monitoringu, je potrebné dodržiavať minimálne nasledujúce zásady:

- musí byť k dispozícii podrobný popis všetkých údajov, ktoré sa zaznamenávajú, ako sa zaznamenávajú, na akú dobu sa uchovávajú a ako sa ďalej používajú,

- musí byť podrobne popísaný prístupový mechanizmus umožňujúci zber údajov (akým spôsobom sa údaje do monitoringu zo zdrojov získavajú),
- musí existovať odôvodnenie, prečo sa údaje z daných zdrojov zaznamenávajú a čo by ukončenie zberu informácií z daného zdroja znamenalo (aké sú dôsledky a riziká ukončenia monitoringu z daného zdroja – napr., ak sa ukončí monitorovanie pracovných staníc, zvýši sa pravdepodobnosť, že dôkazy pre vyšetrenie incidentu nebudú dostatočné a v prípade trestného činu nebude možné tento relevantne dokázať),
- musí byť stanovený a schválený postup pre overovanie fungovania bezpečnostného monitoringu, ktorý bude následne formou kontrol vykonávaný, overovanie musí zahŕňať preskúmavanie/kontrolu aj z pohľadu etických štandardov,
- stratégie zberu informácií do bezpečnostného monitoringu, ako aj samotného fungovania bezpečnostného monitoringu musia byť v pravidelných intervaloch prehodnocované.

6.4 Etické štandardy pri riešení kybernetických bezpečnostných incidentov

Bezpečnostný špecialista alebo tím bezpečnostných špecialistov pri riešení kybernetických bezpečnostných incidentov prichádza do styku s citlivými informáciami alebo údajmi, klasifikovanými informáciami, prípadne informáciami spadajúcimi pod kategóriu osobných údajov (osobné údaje alebo osobitná kategória osobných údajov ako zdravotný záznam), a preto by mal dodržiavať minimálne nasledovné etické štandardy:

- etické štandardy platné pri postupe zabezpečovania dôkazov (napr. existujúce etické štandardy pre forenzných analytikov),
- zachovávanie autenticity a nezmeniteľnosti dôkazov pri získavaní, ukladaní, prenášaní a archivovaní dôkazov,
- dodržiavanie mlčanlivosti a nezdieľania informácií alebo postupov,
- pri zdieľaní informácií dodržiavať princíp „need to know“.

6.5 Etické štandardy pri bezpečnostných testoch alebo penetračnom testovaní

6.5.1 Etické kódexy a audítorské štandardy pre penetračné testy v USA a Spojenom kráľovstve

Spojené štáty americké

V USA sa etické kódexy a audítorské štandardy pre penetračné testy riadia predovšetkým smernicami a nariadeniami stanovenými Národným inštitútom pre štandardy a technológie (NIST), Medzinárodnou organizáciou pre štandardizáciu (ISO) a Asociáciou Auditu a Kontroly Informačných Systémov (ISACA). Niektoré z kľúčových etických kódexov a štandardov pre penetračné testovanie v USA zahŕňajú:

Špeciálna publikácia NIST 800-115: Táto publikácia poskytuje návod na vykonávanie penetračného testovania a hodnotenia zraniteľnosti v súlade s federálnymi požiadavkami pre bezpečnosť informačných systémov.

ISO/IEC 27001: Táto norma poskytuje rámec pre systémy riadenia informačnej bezpečnosti vrátane požiadaviek na penetračné testovanie.

Etický kódex ISACA: Etický kódex ISACA poskytuje návod na profesionálne správanie vrátane etických úvah pri vykonávaní penetračných testov a hodnotení zraniteľnosti.

Spojené kráľovstvo

V Spojenom kráľovstve sa etické kódexy a štandardy auditu pre penetračné testovanie riadia predovšetkým smernicami a nariadeniami stanovenými Národným centrom pre kybernetickú bezpečnosť (NCSC) a organizáciou Chartered Institute of Information Security Professionals (CIISP). Niektoré z kľúčových etických kódexov a noriem pre penetračné testovanie vo Veľkej Británii zahŕňajú:

Rámec penetračného testovania NCSC: Tento rámec poskytuje návod na vykonávanie penetračného testovania v súlade s vládnymi normami a požiadavkami Spojeného kráľovstva.

Kódex správania CREST pre penetračné testovanie: Tento kódex správania poskytuje etické pokyny na vykonávanie penetračných testov vrátane požiadaviek na transparentnosť, informovaný súhlas a rešpektovanie súkromia.

Etický kódex CIISP: Etický kódex CIISP poskytuje návod na profesionálne správanie vrátane etických úvah pri vykonávaní penetračných testov a hodnotení zraniteľnosti.

Etické kódexy a audítorské štandardy pre penetračné testovanie sa môžu líšiť v závislosti od odvetvia, organizácie a krajiny. Pri vykonávaní penetračného testu je dôležité konzultovať štandardy a smernice špecifické pre dané odvetvie, ako aj právne a etické požiadavky.

6.5.2 Návrh prístupu k etickým štandardom

Bezpečnostný špecialista alebo tím bezpečnostných špecialistov pri vykonávaní bezpečnostných testov alebo penetračných testov prichádza do styku s citlivými informáciami alebo údajmi, klasifikovanými informáciami, prípadne informáciami spadajúcimi pod množinu osobných údajov (osobné údaje alebo osobitná kategória osobných údajov ako zdravotný záznam), a preto by mal by mal dodržiavať minimálne nasledovné etické štandardy:

a) Penetračné alebo iné bezpečnostné testovanie vykonáva len na základe platnej zmluvy alebo iného právneho aktu (napríklad predpis, právny úkon ako dohoda alebo súhlas) a iba na základe výslovného súhlasu dotknutej strany, pričom sa striktne drží stanovených postupov (ak sú uvedené v predpise, zmluve alebo inom akte). Rovnako sa drží stanoveného predmetu bezpečnostného auditu alebo penetračného testovania, čo do skúmaného informačného systému/systémov (zameriava sa výlučne na IS a služby, ktoré sú definované v zmluve alebo predpise), ako aj definovanej skupiny informácií alebo údajov (skúmajú sa informácie a skupiny údajov v daných IS a službách).
b) V prípade, že to nie je výslovne uvedené v zmluve alebo predpise, bezpečnostné testovanie alebo útočenie spôsobujúce obmedzenie alebo zastavenie služby alebo IS (DoS, DDoS, „zhodenie“ systému alebo komponentu pretečením /zásobníka pamäte/buffera a pod.) sa nevykonáva.

c) Bezpečnostné testovanie alebo útočenie na IS alebo služby, ktoré môže spôsobiť poškodenie zdravia alebo ohrozenie ľudského života, prípadne spôsobiť hospodárske škody akéhokoľvek rozsahu, je zakázané.
d) Bezpečnostné testovanie alebo útočenie spôsobujúce fyzické poškodenie hardvéru IS, alebo podporných komponentov, prípadne iných aktív testovaného subjektu alebo inej tretej strany (napríklad poškodenie prehriatím, spustenie požiarneho systému a pod.) sa nevykonáva.
e) Zistené bezpečnostné nedostatky, zraniteľnosti, bezpečnostné diery v IS OVM by mali komunikovať len s vlastníkom daného IS alebo s príslušnou autoritou na riešenie incidentov, zraniteľností a pod., pričom autoritou sa myslí SK-CERT alebo príslušný CSIRT (napr. Vládna jednotka CSIRT).
f) Zverejnenie zistených bezpečnostných nedostatkov, zraniteľností alebo bezpečnostných dier, prípadne postupov na získanie informácií v týchto systémoch alebo získanie neoprávnených privilegovaných alebo neprivilegovaných prístupových práv v IS OVM možno realizovať až po výslovnom písomnom súhlase vlastníka IS alebo aplikácie.
g) V prípade, že zistené bezpečnostné nedostatky, zraniteľnosti, bezpečnostné diery v IS, prípadne postupy na získanie informácií v týchto systémoch alebo získanie neoprávnených privilegovaných alebo neprivilegovaných prístupových práv v IS môžu spôsobiť ohrozenie iných IS ako testovanej organizácie, túto skutočnosť bezpečnostný špecialista alebo bezpečnostný tím komunikuje so zástupcami SK-CERT alebo príslušným CSIRT-om a riadi sa ich pokynmi.
h) Bezpečnostný špecialista alebo bezpečnostný tím by od vlastníka dotknutého IS alebo služby, ktorého sa zistené bezpečnostné nedostatky, zraniteľnosti, bezpečnostné diery v IS, prípadne postupy na získanie informácií v týchto IS alebo získanie neoprávnených privilegovaných alebo neprivilegovaných prístupových práv týkajú, nemal žiadať priamu alebo nepriamu kompenzáciu (napríklad finančnú). Taktiež nesmie tieto informácie za poplatok sprístupniť akýmkoľvek iným osobám alebo tretím stranám (napr. na čiernom trhu).
i) Bezpečnostný špecialista alebo bezpečnostný tím by po zistení zraniteľnosti mal poskytnúť vlastníkovi daného IS, služby alebo aplikácie čo najpresnejšie detaily o odhalenom bezpečnostnom probléme – to znamená typ zraniteľnosti, popis konfigurácie, pri ktorej sa dá problém zreprodukovať, prípadne “proof-of-concept” demonštrácia zneužitia (tzv. exploit), ako aj prípadný popis dopadu potenciálneho zneužitia útočníkom.
j) Bezpečnostný špecialista alebo bezpečnostný tím zistené bezpečnostné nedostatky, zraniteľnosti, bezpečnostné diery v IS, prípadne postupy na získanie informácií v týchto systémoch alebo získanie neoprávnených privilegovaných alebo neprivilegovaných prístupových práv publikuje na verejných diskusných fórach, či bezpečnostných konferenciách až po súhlase správcu alebo vlastníka IS, služby alebo aplikácie. Rovnako sa tento postup zverejnenia týka aj výrobcu alebo kľúčového dodávateľa dotknutej technológie alebo operačného systému.

6.5.3 Právne a etické súvislosti pri penetračnom testovaní

Právne a etické súvislosti - sú dôležitým aspektom penetračného testu, pretože zabezpečujú, že proces testovania prebieha zodpovedným spôsobom a v súlade s predpismi. Právne a etické hľadiská pomáhajú zabezpečiť, aby boli rešpektované práva jednotlivcov a organizácií a aby proces testovania nespôsobil škodu alebo neporušil žiadne zákony alebo nariadenia. Niekoľko bežných právnych a etických úvah pre penetračný test zahŕňa:

Súlad s príslušnými zákonmi a nariadeniami - zabezpečenie toho, aby bol penetračný test v súlade s príslušnými zákonmi o ochrane osobných údajov, zákonmi o ochrane údajov a inými predpismi, ktoré sa môžu uplatňovať v jurisdikcii, v ktorej sa test vykonáva.

Súhlas a autorizácia - získanie riadneho súhlasu a autorizácie od všetkých strán zapojených do penetračného testu, vrátane testovanej organizácie, jednotlivcov, ktorých informácie sa získavajú, a akýchkoľvek iných relevantných zainteresovaných strán.

Ochrana údajov - zabezpečenie toho, aby sa s citlivými informáciami a osobnými údajmi zaobchádzalo a spracovávali bezpečným a zodpovedným spôsobom a aby boli zavedené vhodné bezpečnostné opatrenia na ochranu pred neoprávneným prístupom, zneužitím alebo krádežou informácií.

Rešpektovanie práv jednotlivcov - rešpektovanie súkromia a bezpečnosti jednotlivcov, ktorých informácie sa získavajú počas penetračného testu, a zabezpečenie toho, aby sa všetky zhromaždené alebo spracované informácie použili len na účely testu.

Zodpovednosť za neúmyselné následky - prevzatie zodpovednosti za akékoľvek neúmyselné dôsledky, ktoré môžu vyplynúť z penetračného testu, ako je výpadok systému alebo siete, a zabezpečenie prijatia vhodných opatrení na zmiernenie takýchto rizík.

Pri príprave zmluvy o poskytnutí penetračného testu je dôležité konzultovať s právny tímom, aby sa zabezpečilo, že všetky právne aspekty budú primerane vyriešené.

6.6 Základ pre tvorbu štandardov uplatňovaných pri výbere dodávateľa, služby a technológie

Zamestnanec špecifikuje výber danej technológie alebo služby prostredníctvom jej parametrov a zároveň dodržiava pravidlá tak, aby

- zodpovedali platným technickým a technologickým štandardom definovaným v platnej legislatíve SR a EÚ,
- bola dosiahnutá požadovaná úroveň dostupnosti, dôvernosti, integrity a autentickosti informácií a údajov,
- bolo zabezpečené pokrytie licenciami s ohľadom na plánovanú dobu poskytovania služby alebo životný cyklus IS,
- zabezpečenie ochrany osobných údajov bolo v súlade s požiadavkami platnej legislatívy SR a EÚ,
- zabezpečenie mlčanlivosti a ochrany autorských práv bolo zaistené v zmysle požiadaviek platnej legislatívy SR,
- zabezpečenie dodržiavania bezpečnostných opatrení a notifikačných povinností bolo zaistené podľa platnej legislatívy SR a EÚ,
- príslušné bezpečnostné povedomie a bezpečnostné previerky (organizácie/spoločnosti a/alebo jej zamestnancov) zodpovedali kategórii, v ktorej sú údaje alebo informácie klasifikované,
- v rámci požiadaviek na bezpečnostné opatrenia a notifikačné povinnosti sa musí vyžadovať primeraná reakčná doba odpovede ako aj vyriešenia/uzatvorenia problému, pokiaľ pôjde o kybernetický bezpečnostný incident podľa vyhlášky č. 165/2018.

Zamestnanec rešpektuje a dodržiava pravidlá integrity, predchádzania korupcii a konfliktu záujmov a pravidlá spravodlivej hospodárskej súťaže, v zmysle ktorých je zakázané, napríklad:

- prijímať symbolické príležitostné alebo reklamné dary,
- prijímať pozvania na obchodné obedy a večere,
- prijímať pozvania na iné podujatia, ktoré majú za cieľ nečestným spôsobom ovplyvniť obchodné rozhodnutia,
- umožniť technologické, cenové alebo kapacitné zvýhodňovane vybraných dodávateľov,
- vypracovať falošné ponuky vo výberových konaniach stavané na mieru vopred určeného dodávateľa,
- umožniť dodávateľovi využitie dominantného postavenia na trhu.

OVM:

- zabezpečí, aby nielen dodávatelia, ale aj ich subdodávatelia, prijali a zaviedli v rámci svojich obchodných vzťahov/operácií etické štandardy, resp. etický kódex daného OVM,
- je povinný zdržať sa akejkoľvek formy korupcie alebo aktivít, ktoré by za korupciu mohli byť považované (dodržiava protikorupčné zásady s rešpektovaním právnych predpisov, ako napr. Trestnoprávny dohovor o korupcii (oznámenie č. 375/2002 Z. z.) platný pre SR od 1. júla 2002, Dohovor OSN proti korupcii prijatý 31.októbra 2003 v New Yorku, platný pre SR od 1. júla 2006, (oznámenie č. 434/2006 Z. z.), Zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov, Zákon č. 91/2016 Z. z. o trestnej zodpovednosti právnických osôb a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, Zákon č. 315/2016 Z. z. o registri partnerov verejného sektora a o zmene a doplnení niektorých zákonov).

Dodávatelia ďalej napr.:

- musia chrániť dôverné informácie, plniť požiadavky bezpečnostných noriem, zásad a kontrol, dodržiavať zásady uchovávania dokumentov,
- nesmú poskytovať prístup k informáciám OVM bez legitímneho obchodného dôvodu a povolenia osoby zodpovedného vlastníka,
- dbajú o ochranu osobných údajov z pohľadu aktuálnej právnej úpravy ochrany osobných údajov.

6.7 Základ pre tvorbu štandardov uplatňovaných pri výbere bezpečnostných špecialistov pri prijímaní do zamestnania

Pri prijímaní do zamestnania sa organizácie a inštitúcie spadajúce pod verejnú správu riadia samostatnou legislatívou (najmä Zákona č. 55/2017 Z. z., Zákona č. 552/2003 Z. z. a ich vykonávacích predpisov), pričom je vyžadovaná najmä trestná bezúhonnosť (overovaná počas prijímacieho procesu).

Ďalšie pravidlá sa majú týkať odbornosti a absolvovanej praxe v danom obore, pod ktorý daná bezpečnostná rola spadá.

V niektorých špecifických prípadoch sa môže vykonať analýza správania sa zamestnancov zastávajúcich niektorú z bezpečnostných rolí na sociálnych sieťach (Facebook, LinkedIn, verejné a diskusné fóra a pod.). V týchto prípadoch sa však musí vykonať dodatočná analýza dopadov na zásah do ľudských práv (tzv. Posúdenie vplyvu, viď. Nariadenie GDPR) a podobne.

V rámci výberového konania na pozície bezpečnostných špecialistov jednou z oblastí výberového procesu musí byť aj overovanie uchádzačov z pohľadu etických štandardov, pričom je potrebné najmä:

- dodržiavať platné zákonné a legislatívne úpravy,
- overiť predchádzajúce porušenia platných zákonov (odpisom alebo výpisom z registra trestov, v zmysle platnej legislatívy),
- overiť predchádzajúce porušenie etických zásad (odobratie/strata certifikátu následkom porušenia etických štandardov organizácie, rozviazanie predchádzajúceho pracovného pomeru na základe porušenia etických štandardov, ku ktorým bola dotknutá osoba zaviazaná),
- overiť si znalosť princípov etických štandardov na vzorovej modelovej situácii na pracovnom pohovore,
- overiť ochotu dodržiavať etické štandardy v danej pracovnej pozícii, napríklad podpisom záväzku dodržiavať etický kódex.

  Pri skúmaní vyššie uvedeného je nevyhnutné rešpektovať dôstojnosť a ľudské práva každého z uchádzačov.

6.8 Ďalšie doplňujúce ustanovenia

- Etický kódex a jeho ustanovenia sú záväzné pre všetkých zamestnancov OVM v sektore ITVS.
- Akékoľvek porušenie tohto kódexu môže byť podľa svojej závažnosti alebo frekvencie výskytu dôvodom na udelenie sankcie, ktorou môže byť až ukončenie pracovného pomeru zo strany zamestnávateľa.
- Ten, kto podá zámerne falošné oznámenie o porušení etického kódexu s cieľom poškodiť iného, sám sa dopúšťa porušenia etického kódexu.
- OVM využíva primerané technické a organizačné prostriedky, aby ochránil údaje o organizácii, zákazníkoch, obchodných partneroch, občanoch a zamestnancoch pred neoprávneným prístupom, nepovoleným využívaním, zneužitím, odcudzením a predčasným zničením.
- K ochrane údajov sa pristupuje v súlade s príslušnými právnymi požiadavkami a zákonmi, ako aj internými smernicami a usmerneniami.
- Pri nástupe do zamestnania je vhodné vyžadovať od nastupujúceho zamestnanca podpísanie dokumentu, v ktorom potvrdzujú oboznámenie sa so stanoveným etickým kódexom.
- Zamestnanci sa podpisom etického kódexu zaväzujú k jeho dodržiavaniu a potvrdzujú, že preberajú na seba zodpovednosť v prípade jeho porušenia.
- Etický kódex možno kedykoľvek meniť, ako živý dokument, ktorý sa prispôsobuje meniacim sa výzvam bezpečnosti v sektore ITVS; možnosti zmeny a oboznamovania so zmenami je vhodné osobitne upraviť v samotnom etickom kódexe.

7 Usmernenie pri tvorbe etických kódexov v podmienkach OVM

Tvorbou konkrétnych etických kódexov je potrebné poveriť (interných alebo externých) odborníkov, ktorí majú skúsenosti s tvorbou etických kódexov.

Východiskom pre tvorbu etických kódexov sú štandardy uvedené v kapitole 5 so zohľadnením základných princípov etického správania (kap. 4). Je však nevyhnutné zohľadniť typ a zameranie OVM, ako aj využívané pozície bezpečnostných špecialistov, resp. bezpečnostných rolí (napr. penetračný tester) a typ bezpečnostných pracovísk definovaných v aktuálne platnej legislatíve a metodických pokynoch vydaných sektorovým ústredným orgánom pre riadenie KB v sektore VS.

Každý OVM by mal

- mať vlastný etický kódex (prevzatý alebo odvodený z výstupov tohto dokumentu) postavený na definovaných etických štandardoch.
- etický kódex publikovať a zverejniť a prípadne deklarovať vo svojich politikách medzi záväzkami.
- oboznámiť zamestnancov so schváleným etickým kódexom a v pravidelných intervaloch ich preukázateľne preškoliť.
- dodržiavanie etického kódexu vyžadovať spôsobom vo forme deklarácie v služobnej/pracovnej zmluve a/alebo podpisom samostatného dokumentu ako záväzku dodržiavať etické štandardy uvedené v kódexe.
- vyžadovať pri nástupe do zamestnania podpísanie záväzku, čím zamestnanec deklaruje, že bude dodržiavať etický kódex.
- na účely kontroly a uplatňovania etického kódexu vytvoriť etickú komisiu alebo obdobný orgán a riešiť porušenia etického kódexu.
- porušenie etického kódexu môže byť považované za porušenie služobnej/pracovnej disciplíny.
- vyžadovať dodržiavanie etického kódexu aj od partnerov, dodávateľov a iných tretích strán (napríklad pri verejnom obstarávaní, či formou osobitného ustanovenia v zmluvách, dodatku k existujúcim zmluvám, a pod.).