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

(1) 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.

(2) 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.

(3) Manažér kybernetickej bezpečnosti podnikne všetky kroky na rozvoj vlastnej odbornej spôsobilosti v súlade s aktuálnym vývojom v profesionálnej oblasti.

(4) Manažér kybernetickej bezpečnosti si uplatní nárok iba na také členstvá a kvalifikácie, ktoré sú v danom čase platné.

(5) 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.

(6) Manažér kybernetickej bezpečnosti musí za každých okolností konať tak, aby zachoval dôstojnosť a dobrú povesť tejto profesie.

(7) Manažér kybernetickej bezpečnosti nebude vedome vykonávať činnosť, pre ktorú nemá dostatočné zručnosti, vedomosti a zodpovedajúcu právomoc.

(8) 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

(1) 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.

(2) Manažér kybernetickej bezpečnosti sa vyhýba takým činnostiam alebo úlohám, ktoré môžu spôsobiť konflikt záujmov pri výkone jeho pracovných zodpovedností.

(3) 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.

(4) 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.

(5) Manažér kybernetickej bezpečnosti nesmie zneužívať svoje postavenie, súvisiace s výkonom jeho činnosti pri uskutočňovaní súkromných záujmov vo vlastný prospech alebo v prospech tretích strán.

(6) 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

(1) 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.

(2) Manažér kybernetickej bezpečnosti sa vyhýba neodôvodnenej negatívnej komunikácii alebo publikovaniu neprimeranej kritiky, v súvislosti s odbornou činnosťou iného manažéra kybernetickej bezpečnosti.

(3) Manažér kybernetickej bezpečnosti nesmie úmyselne dostať kolegu - manažéra kybernetickej bezpečnosti do situácie, v ktorej by mohol nevedomky porušiť niektorú časť tohto etického kódexu.