VOJENSKÝ ÚTVAR 9066
TRENČÍN
Č.: 6.spojp-EL 7/11-1-16/2023

Trenčín, 18. apríl 2023
Výtlačok jediný.
Počet listov: 11

Schvaľujem: _____

Bezpečnostná politika CAMOSR

Spracovateľ: Centrum správy IB a systémov OUS / Úsek PKIaCA
Verzia: 1.0.
Dátum platnosti: 18. APR. 2023

6. spojovací pluk
Olbrachtova 5, 911 01 TRENČÍN
tel.: +421 960 406300
fax.: +421 960 406503
e-mail: pki@mil.sk
web: http://pki.mil.sk

Ochranné známky

Mená produktov uvádzané v tomto dokumente môžu byť registrované ochranné známky príslušných firiem.

História zmien

Verzia	Dátum	Opis revízie
1.0.	30.11.2022	Finálna verzia dokumentu

Obsah

1. Zoznam obrázkov a tabuliek

1.1. Obrázky

Dokument neobsahuje obrázky.

1.2. Tabuľky

Dokument neobsahuje obrázky.

2. Pojmy a skratky

2.1. Pojmy

Aktívum – čokoľvek, čo má pre CAMOSR hodnotu a je to potrebné chrániť. Aktíva informačného systému sú: kľúče, softvér, hardvér, údaje, dokumenty a komunikačné prostriedky, ktoré CAMOSR používa na zabezpečenie poskytovania služieb. Medzi aktíva sa radia aj zamestnanci CAMOSR.

Analýza rizík – proces identifikovania bezpečnostných rizík, ktorý stanovuje ich dôležitosť a identifikuje oblasti vyžadujúce ochranné opatrenia. Ide o preskúmanie vzťahov medzi aktívami, hrozbami, bezpečnostnými slabinami a opatreniami s cieľom určiť aktuálnu úroveň rizík.

Bezpečnostná politika – sú pravidlá, smernice a praktiky, ktoré rozhodujú o tom, ako sú aktíva vrátane citlivých informácií spravované, chránené a distribuované vo vnútri CAMOSR a jej informačnom systéme.

Bezpečnostná slabina – stav zraniteľnosti zapríčinený nedostatkom bezpečnostného opatrenia alebo jeho neprítomnosťou.

Bezpečnostné opatrenie – prax, postup alebo mechanizmus, ktorý znižuje riziko.

Bezpečnostný incident – akákoľvek aktivita používateľa alebo iného subjektu porušujúca všeobecne bezpečnosť informačného systému, konkrétne niektorú zásadu bezpečnostnej politiky alebo niektoré bezpečnostné opatrenie.

Bezpečnosť IT – všetky aspekty súvisiace s definovaním, dosiahnutím a udržovaním dôvernosti, integrity, dostupnosti, individuálnej zodpovednosti, autenticity a spoľahlivosti IT.

Bezpečnostný manažér – je osoba zodpovedná za implementáciu celkovej bezpečnostnej politiky, jej presadzovanie a udržiavanie.

Certifikát pre elektronický podpis – je elektronické osvedčenie, ktoré spája údaje na validáciu elektronického podpisu s fyzickou osobou a potvrdzuje aspoň jej meno alebo pseudonym.

Dostupnosť – vlastnosť, že je niečo (napríklad údaje alebo služby CAMOSR) na požiadanie prístupné a použiteľné oprávnenou entitou.

Dôležité činnosti – činnosti, ktoré sú pre CAMOSR prioritné, ich výpadok vytvára vážne problémy v zabezpečovaní služieb, ktoré má CAMOSR zo zákona vykonávať (napr. pravidelné zverejňovanie CRL prevádzkovanou CAMOSR).

Dôsledok – strata ako výsledok naplnených hrozieb môže byt' vyjadrená prostredníctvom jednej alebo viacerých oblastí dôsledkov. K základným oblastiam patrí zničenie, znemožnenie prístupu k službe, prezradenie a modifikácia.

Dôvernosť – vlastnosť, že informácia nie je dostupná alebo prístupná neoprávneným jednotlivcom, entitám alebo procesom.

Držiteľ – entita identifikovaná v certifikáte ako držiteľ súkromného kľúča prislúchajúceho k verejnému kľúču obsiahnutému v certifikáte.

Elektronický podpis – informácia pripojená alebo inak logicky spojená s elektronickým dokumentom, ktorá obsahuje údaj umožňujúci identifikáciu podpisovateľa.

Hrozba – potenciálna príčina neželanej udalosti, ktorá môže mať za následok poškodenie informačného systému alebo CAMOSR ako celku. Výsledkom hrozby môže byť degradácia: utajenia (kompromitácia), celistvosti (narušenie integrity) alebo dostupnosti (znemožnenie prístupu k službe) systému alebo siete.

Integrita údajov – vlastnosť, že údaje neboli zmenené alebo zničené neoprávneným spôsobom.

Kvalifikovaný elektronický podpis – je zdokonalený elektronický podpis vyhotovený s použitím zariadenia na vyhotovenie kvalifikovaného elektronického podpisu a založený na kvalifikovanom certifikáte pre elektronické podpisy.

Kvalifikovaný poskytovateľ dôveryhodných služieb - poskytovateľ dôveryhodných služieb, ktorý poskytuje kvalifikované dôveryhodné služby podľa 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), a ktorá má na poskytovanie týchto služieb kvalifikáciu Národného bezpečnostného úradu (ďalej len NBÚ).

Poskytovateľ dôveryhodných služieb – poskytovateľ dôveryhodných služieb, ktorý vykonáva dôveryhodné služby spojené s vydávaním, archivovaním, rušením platnosti certifikátov, overovaním ich platnosti a pod.

Používateľ certifikátu – entita, ktorá koná na báze dôvery v daný certifikát a/alebo na základe elektronického podpisu overeného daným certifikátom. Synonymom pojmu používateľ certifikátu je pojem strana spoliehajúca sa na certifikát.

Riadenie informačnej bezpečnosti – postupy založené na prístupe k rizikám CAMOSR, ktorých úlohou je implementovať, prevádzkovať, monitorovať, preskúmavať, udržiavať a zlepšovať informačnú bezpečnosť CAMOSR.

Riziko – potenciálna možnosť, že daná hrozba využije zraniteľnosť aktív alebo skupiny aktív a spôsobí tak stratu alebo zničenie aktív.

Subjekt – entita identifikovaná v certifikáte ako držiteľ súkromného kľúča prislúchajúceho k verejnému kľúču obsiahnutému v certifikáte.

Vlastná CA – časť infraštruktúry poskytovateľa dôveryhodných služieb (obsahujúca napr. HSM modul), ktorá spolu s poskytovateľom vydáva certifikáty.

X.509 - medzinárodný štandard, ktorý okrem iného definuje aj formát certifikátu verejného kľúča.

Zdokonalený elektronický podpis – je elektronický podpis, ktorý spĺňa požiadavky stanovené v článku 26 Nariadenia (EÚ) 910/2014.

Žiadateľ o certifikát – entita, ktorá certifikačnej autorite predkladá žiadosť v mene jedného alebo viacerých subjektov.

2.2. Skratky

BP	–	Bezpečnostná politika
BOZP	–	Bezpečnosť a ochrana zdravia pri práci
CA	–	Certifikačná autorita poskytujúca dôveryhodné služby
CAMOSR	–	Certifikačná autorita poskytujúca dôveryhodné služby pre MOSR
FW	–	Bezpečnostná brána (Firewall)
IDS	–	Systém detekcie prienikov (Intrusion Detection System)
IS	–	Informačný systém
IT	–	Informačné technológie
MOSR	–	Ministerstvo obrany Slovenskej republiky
PMA	–	Autorita pre správu politík (Policy Management Authority)
SIEM	–	Systém riadenia bezpečnostných informácií a udalostí (Security Information and Event Management)
SW	–	Softvér

3. Identifikácia, pôsobnosť a obsah bezpečnostnej politiky

Bezpečnostná politika certifikačnej autority Ministerstva obrany Slovenskej republiky (ďalej len CAMOSR) predstavuje základný dokument riadenia informačnej bezpečnosti informačného systému CAMOSR.

Bezpečnostná politika CAMOSR je spracovaná v súlade s požiadavkami normy STN EN ISO/IEC 27001 a STN EN ISO/IEC 27002 ako vrcholová politika riadenia informačnej bezpečnosti CAMOSR. Bezpečnostná politika CAMOSR zohľadňuje aj požiadavky ochrany osobných údajov v súlade so zákonom č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

Bezpečnostná politika CAMOSR sa vzťahuje na všetky aktíva CAMOSR a kladie bezpečnostné požiadavky na externé systémy, ktoré komunikujú s informačným systémom CAMOSR.

Bezpečnostná politika CAMOSR je verejný dokument a vzťahuje sa na všetkých zamestnancov podieľajúcich sa na poskytovaní kvalifikovaných dôveryhodných služieb CAMOSR v súlade s platnou legislatívou, používateľa certifikátu, dodávateľov a prípadné tretie strany.

Všeobecné ustanovenia bezpečnostnej politiky CAMOSR sú detailne rozpracované v dokumente Pravidlá informačnej bezpečnosti CAMOSR.

4. Deklarácia prevádzkovateľa CAMOSR o podpore a význame informačnej bezpečnosti

Prevádzkovateľ CAMOSR poskytuje dôveryhodné služby pre príslušníkov organizačne patriacich pod Ministerstvo obrany Slovenskej republiky pri implementovaní infraštruktúry verejných kľúčov pozostávajúcej z produktov a služieb, ktoré poskytujú a spravujú kvalifikované certifikáty (ďalej len certifikáty) podľa štandardu X.509 pre kryptografiu verejných kľúčov v súlade so zákonom 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). Certifikáty identifikujú subjekt nachádzajúci sa v certifikáte a zväzujú tento subjekt s príslušným párom kľúčov.

Pri plnení hlavných úloh a zabezpečovaní vlastnej činnosti CAMOSR využíva informácie, ktoré spracováva pomocou informačného systému CAMOSR, počítačových sietí a informačných technológií. Narušenie aktív CAMOSR môže prevádzkovateľa CAMOSR obmedziť pri poskytovaní kvalifikovaných dôveryhodných služieb v súlade so zákonom o dôveryhodných službách.

Popis hrozieb pôsobiacich na aktíva CAMOSR je uvedený v dokumente Pravidlá informačnej bezpečnosti CAMOSR.

Aktíva, ktoré súvisia so spracovaním informácií, sa nazývajú informačné aktíva. Zabezpečenie primeranej ochrany informačných aktív CAMOSR (zaistenie a udržiavanie primeranej úrovne informačnej bezpečnosti) je nutným predpokladom toho, aby CAMOSR mohla poskytovať dôveryhodné služby. Každý, kto má prístup k informačným aktívam CAMOSR, musí dodržiavať ustanovenia bezpečnostnej politiky CAMOSR a podieľať sa spôsobom zodpovedajúcim jeho pracovnému zaradeniu na plnení cieľov informačnej bezpečnosti (Pravidlá informačnej bezpečnosti CAMOSR kapitola 5.1).

Vedenie prevádzkovateľa CAMOSR považuje zaistenie primeranej úrovne informačnej bezpečnosti CAMOSR za trvalú úlohu s najvyššou prioritou a zaväzuje sa na plnenie tejto úlohy vytvárať primerané personálne, organizačné, právne, materiálne, technické aj finančné podmienky.

5. Základné princípy (zásady) informačnej bezpečnosti

Zaisťovanie informačnej bezpečnosti CAMOSR vychádza z nasledujúcich zásad:

a) Používateľ môže informácie, informačné systémy a iné zdroje CAMOSR používať len na plnenie svojich pracovných povinností.
b) Čo nie je povolené to je zakázané.
c) Princíp najnižších oprávnení (least privilege principle). Používateľ má v systéme oprávnenia na najnižšej možnej úrovni postačujúcej na plnenie jeho pracovných úloh.
d) Princíp potreby vedieť (need to know).
e) Princíp potreby používať (need to use).
f) Úroveň ochrany aktív CAMOSR je úmerná významu aktív pre CAMOSR a potenciálnemu dopadu ich narušenia.
g) K informačným aktívam CAMOSR (s výnimkou verejných informácií) nie je možný anonymný prístup.
h) Identita používateľa v systéme je jednoznačne stanoviteľná a každý používateľ zodpovedá za svoje aktivity v systéme.
i) Činnosti, pri ktorých by mohlo dôjsť ku konfliktu nezlučiteľnosti rolí, nesmie vykonávať jedna osoba (separation of duties).
j) Princíp štyroch očí pre dôležité operácie poskytovania dôveryhodných služieb.

6. Riadenie informačnej bezpečnosti

Informácie, informačné systémy, počítačové siete a ďalšie informačné aktíva, ktoré CAMOSR využíva na poskytovanie dôveryhodných služieb v súlade so zákonom o dôveryhodných službách tvoria informačný systém CAMOSR.

Prevádzkovateľ CAMOSR zaviedol systém riadenia informačnej bezpečnosti CAMOSR v súlade s normou STN EN ISO/IEC 27001.

Každá osoba, ktorá môže svojím konaním ovplyvniť informačnú bezpečnosť CAMOSR, je povinná dodržiavať ustanovenia tejto Bezpečnostnej politiky CAMOSR a dokumentov, v ktorých sú ustanovenia tejto politiky detailnejšie rozpracované. Zamestnanci prevádzkovateľa CAMOSR podieľajúci sa na poskytovaní kvalifikovaných dôveryhodných služieb musia byť zaradení aspoň do jednej z bezpečnostných rol. Bezpečnostné roly špecifikujú oprávnenia a povinnosti, ktoré osoba zaradená do danej roly má vo vzťahu k informačným aktívam CAMOSR a vzťahy s inými bezpečnostnými rolami.

CAMOSR má definované tieto bezpečnostné roly:

a) autorita pre správu politík – PMA,
b) hlavný bezpečnostný manažér,
c) bezpečnostný manažér IDS,
d) bezpečnostný manažér FW,
e) interný audítor,
f) administrátor certifikačnej autority,
g) systémový administrátor,
h) operátor certifikačnej autority,
i) operátor registračnej autority.

Oblasť riadenia informačnej bezpečnosti je podrobne opísaná v dokumente Pravidlá informačnej bezpečnosti CAMOSR.

7. Základný rámec riadenia aktív

Informačná bezpečnosť prevádzkovaných kvalifikovaných dôveryhodných služieb CAMOSR sa zabezpečuje v celom ich životnom cykle od vývoja, nasadenia, prevádzky až po ich likvidáciu. Adekvátne bezpečnostné opatrenia je potrebné zabezpečiť nielen v prevádzkovom prostredí ale aj v testovacom a záložnom prostredí.

Na určenie spôsobu ochrany informácií musí byť vypracovaná klasifikačná schéma zohľadňujúca dôvernosť, integritu a dostupnosť údajov a na základe klasifikácie musia byť stanovené bezpečnostné požiadavky pre všetky aktíva informačného systému CAMOSR.

Ochrana informačného systému CAMOSR musí byť riešená ochranou do hĺbky kombináciou prevenčných, detekčných a eliminačných opatrení.

Ochrana aktív pri spracovávaní informácií v informačnom systéme CAMOSR sa zabezpečuje:

a) implementáciou nástrojov pre ochranu proti škodlivému softvéru,
b) ochranou webovej aplikácie na základe filtrov webovej komunikácie,
c) prenosom údajov na úrovni point-to-point tak, aby nedošlo k narušeniu dôvernosti a integrity klasifikovaných údajov pri prenose,
d) prenosom údajov tak, aby bolo možné overiť zachovanie ich integrity po prenose,
e) segmentáciou prostredia do bezpečnostných zón na úrovni siete s definovanými prestupnými bodmi medzi zónami,
f) monitorovaním bezpečnosti informačných systémov a sietí prostredníctvom nástroja SIEM, ktorý zahŕňa minimálne: vstupný perimeter, prístupy používateľov a aktivity správcov systému,
g) konfiguráciou databázy a dátového úložiská tak, aby aj pri využití, zneužití či kompromitácii prístupových práv oprávnených osôb bolo riziko úniku údajov čo najmenšie.

Oblasť riadenia aktív je podrobne opísaná v dokumente Pravidlá informačnej bezpečnosti CAMOSR.

8. Základný rámec riadenia rizík

Základný rámec riadenia rizík je založený na:

a) identifikácii aktív,
b) identifikácii hrozieb,
c) analýze a hodnotení rizík,
d) formulácii bezpečnostných opatrení,
e) implementácii bezpečnostných opatrení a ich správy,
f) monitorovaní bezpečnosti a hodnotení stavu informačnej bezpečnosti,
g) audite bezpečnosti.

Výdavky na bezpečnostné opatrenia musia korešpondovať potenciálnym stratám v dôsledku výskytu rizík (finančne alebo iným spôsobom kvantifikovateľným) a musia byť schválené PMA.

Celý proces hodnotenia rizík musí prebiehať na viacerých úrovniach a v miere detailu, ktorá zodpovedá závažnosti hroziacich bezpečnostných incidentov. Oblasť riadenia rizík je podrobne opísaná v dokumente Pravidlá informačnej bezpečnosti CAMOSR.

9. Personálna bezpečnosť

Bezpečnosť aktív CAMOSR môže pozitívne alebo negatívne ovplyvniť každá osoba, ktorá k nim má prístup. Používanie aktív CAMOSR vychádza z princípov potreby vedieť (need to know) a potreby používať (need to use). Zamestnanec môže používať len tie aktíva CAMOSR, ktoré potrebuje na výkon pracovných povinností a spôsobom, ktorý je nevyhnutný na plnenie stanovených úloh. Tieto zásady sa premietajú do opatrení personálnej bezpečnosti, ktoré sa vzťahujú na všetkých zamestnancov, externých spolupracovníkov a primerane na zamestnancov tretích strán, spolupracujúcich s CAMOSR a platia minimálne po dobu trvania pracovného vzťahu a prípadne aj po ňom.

Oblasť personálnej bezpečnosti je podrobne opísaná v dokumente Pravidlá informačnej bezpečnosti CAMOSR.

10. Klasifikácia informácií

Úroveň ochrany informačných aktív CAMOSR je úmerná ich významu a spôsob ochrany bezpečnostným potrebám jednotlivých aktív. Tie sa rámcovo stanovujú pomocou bezpečnostnej klasifikácie informácie.

Oblasť klasifikácie informácií je podrobne opísaná v dokumente Pravidlá informačnej bezpečnosti CAMOSR.

11. Riadenie prístupu

Práca s aktívami si vyžaduje, aby k nim mal používateľ prístup logický, prostredníctvom procesu, ktorý iniciuje alebo fyzický. Interakcia s aktívami je nevyhnutná na plnenie pracovných povinností, ale predstavuje aj hrozbu, ak používateľ narába s aktívami iným ako povoleným spôsobom. Riadenie prístupu k aktívam CAMOSR je jeden zo základných prvkov informačnej bezpečnosti.

Cieľom riadenia prístupu v informačnom systéme CAMOSR je obmedziť prístup k aktívam CAMOSR a znížiť tak riziko toho, že s nimi bude môcť manipulovať neoprávnená osoba.

V informačnom systéme CAMOSR sa uplatňuje princíp minimálnych privilégií, t.j. človek bude mať prístup len k tým aktívam, ktoré potrebuje na plnenie svojich povinností a v potrebnom rozsahu. Anonymný prístup je povolený len k verejne dostupným informáciám. Pri všetkých aktivitách v systéme musí byť možnosť určiť osobu, ktorá ich vykonala.

Prevádzkovateľ CAMOSR zavedie, zdokumentuje a bude pravidelne revidovať postupy riadenia prístupu, ktoré budú rovnako zohľadňovať potreby CAMOSR ako aj bezpečnostné požiadavky. Vlastníci aktív stanovia pre svoje aktíva pravidlá riadenia prístupu, oprávnenia a obmedzenia prístupu, ktoré sú viazané na jednotlivé bezpečnostné roly.

Prevádzkovateľ CAMOSR zavedie formálny proces správy používateľov, aby zaistil oprávneným používateľom prístup k aktívam a zamedzil ho neoprávneným osobám. Každému používateľovi bude v informačnom systéme CAMOSR pridelený jedinečný identifikátor, prostredníctvom ktorého ho bude možné jednoznačne identifikovať. Používanie skupinových identifikátorov v informačnom systéme CAMOSR musí byť zdôvodnené, povolené a zdokumentované. Prístup jednotlivcov ku skupinovým identifikátorom je riadený rovnakými pravidlami riadenia prístupu ako aktíva, ku ktorým skupinový identifikátor umožňuje prístup.

Prideľovanie privilegovaných prístupových práv je v informačnom systéme CAMOSR obmedzené a podlieha formálnemu schvaľovaciemu procesu.

Na overenie identity (autentifikáciu) používateľa sa v informačnom systéme CAMOSR používajú čipové karty. Používatelia sú povinní neustále chrániť svoje privátne kľúče, čipovú kartu a heslo na prístup k týmto privátnym kľúčom, aby nedošlo k ich zneužitiu . V prípade straty čipovej karty, zneužitia alebo kompromitácie privátneho kľúča alebo zabudnutia hesla na prístup k privátnemu kľúču bezodkladne požiadať o zrušenie daného certifikátu. Ak používateľ nenahlási a primerane neadresuje túto skutočnosť, nesie zodpovednosť za prípadnú škodu spôsobenú týmto únikom.

Oblasť riadenia prístupu je podrobne opísaná v dokumente Pravidlá informačnej bezpečnosti CAMOSR.

12. Riadenie bezpečnostných incidentov

Cieľom tejto časti bezpečnostnej politiky CAMOSR je zaistiť konzistentný a efektívny prístup k riadeniu bezpečnostných incidentov, vrátane oznamovania bezpečnostne relevantných udalostí a možných zraniteľností.

Bezpečnostne relevantná udalosť je udalosť, ktorá môže mať negatívny dopad na aktíva CAMOSR, bezpečnostný incident je udalosť, ktorá má negatívny dopad na aktíva CAMOSR.

Každý zamestnanec CAMOSR a v primeranej miere externý spolupracovník a zamestnanec tretej strany je povinný:

a) dodržiavať ustanovenia tejto politiky a dokumentov, v ktorých je detailnejšie rozpracovaná, aby svojím konaním nespôsobil bezpečnostný incident,
b) upozorniť na potenciálnu zraniteľnosť alebo bezpečnostne relevantnú udalosť, ktorú spozoroval,
c) podieľať sa na riešení bezpečnostného incidentu podľa pokynov osoby, ktorá riadi riešenie daného bezpečnostného incidentu.

Prípravu na riešenie bezpečnostných incidentov ako aj samotné riešenie bezpečnostných incidentov v informačnom systéme CAMOSR koordinuje hlavný bezpečnostný manažér.

Oblasť riadenia bezpečnostných incidentov je podrobne opísaná v dokumente Pravidlá informačnej bezpečnosti CAMOSR.

13. Riadenie kontinuity činnosti

Prevádzkovateľ CAMOSR má zavedený systém riadenia kontinuity činnosti, ktorého úlohou je zvyšovať odolnosť poskytovaných kvalifikovaných dôveryhodných služieb, ktoré sú z časového hľadiska kritické, adekvátne reagovať na bezpečnostné incidenty, ktoré ich narušujú a obnoviť činnosti v čo najkratšom čase.

Oblasť riadenia kontinuity činnosti je podrobne opísaná v dokumente Pravidlá informačnej bezpečnosti CAMOSR.

14. Riadenie zmien

14.1. Aktualizácia bezpečnostnej stratégie

Bezpečnostná politika CAMOSR predstavuje základný dokument navrhnutý tak, aby nepodliehal častým zmenám. Čiastkové zmeny v návrhu informačného systému CAMOSR sa premietnu hlavne v jednotlivých dokumentoch, popisujúcich konkrétne pravidlá, postupy, zodpovednosti a činnosti zodpovedných zamestnancov.

14.2. Súvisiaca dokumentácia

Základom bezpečnostnej dokumentácie CAMOSR je súbor politík, smerníc, postupov, nariadení a riadiacich aktov, ktoré obsahujú platné pravidlá, postupy a popisy riešení reprezentujúce realizované bezpečnostné opatrenia, ktoré zaisťujú adekvátnu ochranu informácií spracovávaných informačným systémom CAMOSR. Súvisiaca dokumentácia, uvedená v tejto bezpečnostnej politike je dlhodobá, záväzná a platná po schválení.

14.3. Revízia a hodnotenie

Každý dokument bezpečnostnej dokumentácie má určenú osobu, ktorá je zodpovedná za jeho vznik, formálnu a obsahovú správnosť a aktuálnosť. Každá nová verzia dokumentu musí byť schválená zodpovednými zamestnancami CAMOSR.

Garantom tohto dokumentu je vedúci CAMOSR.

Garantov pre jednotlivé dokumenty menuje vedúci CAMOSR, ktorý je tiež zodpovedný za zabezpečenie dostupnosti platnej verzie všetkým zamestnancom CAMOSR, ktorých sa dokument dotýka.

14.4. Sankcie a postihy

Porušenie zásad, stanovených touto bezpečnostnou politikou zo strany zamestnanca, bude posudzované ako závažné porušenie pracovnej disciplíny a zamestnanec bude riešený v zmysle Pracovného poriadku Ministerstva obrany Slovenskej republiky, Generálneho štábu Ozbrojených síl Slovenskej republiky a Ozbrojených síl Slovenskej republiky v znení neskorších dodatkov a zákona č. 311/2001 Z.z. Zákonníka práce v znení neskorších predpisov.

Porušením zásad zo strany profesionálneho vojaka, stanovených touto bezpečnostnou politikou, sa profesionálny vojak dopustí disciplinárneho previnenia a bude riešený za porušenie základných povinností profesionálneho vojaka v zmysle zákona č. 281/2015 Z.z. o štátnej službe profesionálnych vojakov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

14.5. Výnimky

Pokiaľ nastane situácia, kedy bude potrebné udeliť výnimku zo zavedených bezpečnostných pravidiel a zásad, ktoré sú dané platnou bezpečnostnou politikou, musí byť táto výnimka odborne posúdená zodpovedným zamestnancom, schválená vedúcim CAMOSR a odpovedajúcim spôsobom zdokumentovaná.

15. Odkazy

Ako legislatívne východiská slúžia nasledovné zákony:

- Zákon 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),
- Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES, Nariadenie (EÚ) č. 910/2014 a Korigendum.
- Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.
- Nariadenie 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).

Ďalšie dokumenty použité pri tvorbe bezpečnostnej politiky:

- STN EN ISO/IEC 27001 - Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Požiadavky (ISO/IEC 27001:2013 vrátane Cor. 1: 2014 a Cor. 2: 2015),
- STN EN ISO/IEC 27002 - Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti (ISO/IEC 27002:2013 vrátane Cor. 1: 2014 a Cor. 2: 2015).
- IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and certification Practices Framework, pozri https://tools.ietf.org/html/rfc3647.
- Recommendation ITU-T X.509 | ISO/IEC 9594-8 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, pozri http://www.itu.int/itu-t/recommendations/rec.aspx?rec=X.509.