VOJENSKÝ ÚTVAR 9066
TRENČÍN
Č.: 6.spojp-EL 7/11-1-17/2023

Trenčín, 18. apríl 2023
Výtlačok jediný.
Počet listov: 9

Schvaľujem: _____

Bezpečnostná stratégia 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.	19.07.2022	Finálna verzia dokumentu

Obsah

1. Zoznam obrázkov a tabuliek

1.1. Obrázky

Dokument neobsahuje obrázky.

1.2. Tabuľky

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 a komunikačné prostriedky, ktoré CAMOSR používa na zabezpečenie poskytovania kvalifikovaných dôveryhodných 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.

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.

Hrozba – potenciálna príčina neželanej udalosti, ktorá môže mať za následok poškodenie informačného systému alebo CAMOSR ako celku. Výsledkom hrozby môže byt'

degradácia: utajenia (kompromitácia), celistvosti (narušenie integrity) alebo dostupnosti (znemožnenie prístupu k službe) systému alebo siete.

Informačná bezpečnosť – súbor aspektov týkajúcich sa dosiahnutia a udržiavania dôvernosti, integrity a dostupnosti informačných aktív.

Informačné aktívum – hmotné alebo nehmotné aktívum súvisiace s informáciami informačného systému ako napr. údaj, programové vybavenie, dokumentácia k systémom, zmluvy a pod.

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

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.

2.2. Skratky

BP	–	Bezpečnostná politika
BOZP	–	Bezpečnosť a ochrana zdravia pri práci
CA	–	Certifikačná autorita poskytujúca dôveryhodné služby
CAMOSR	–	Certifikačná autorita poskytujúca kvalifikované 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)

3. Identifikácia dokumentu a rozsah platnosti

Bezpečnostná stratégia certifikačnej autority Ministerstva obrany Slovenskej republiky (ďalej len CAMOSR) predstavuje základný dokument riadenia informačnej bezpečnosti informačného systému CAMOSR. Definuje základné oblasti informačnej bezpečnosti pre zabezpečenie ochrany aktív CAMOSR.

Bezpečnostná stratégia CAMOSR je spracovaná v súlade s požiadavkami normy STN EN ISO/IEC 27001 a STN EN ISO/IEC 27002 ako vrcholový dokument riadenia informačnej bezpečnosti CAMOSR.

Bezpečnostná stratégia 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.

Riadenie informačnej bezpečnosti CAMOSR sa zabezpečuje prostredníctvom:

a) spracovania a zavedenia bezpečnostnej stratégie CAMOSR,
b) spracovania a zavedenia bezpečnostnej politiky CAMOSR,
c) spracovania a zavedenia pravidiel informačnej bezpečnosti CAMOSR,
d) zaistenia toho, aby boli stanovené ciele informačnej bezpečnosti,
e) ustanovenia rolí a zodpovedností za informačnú bezpečnosť,
f) oboznámenia zamestnancov CAMOSR o dôležitosti plnenia cieľov informačnej bezpečnosti, dodržiavania riadiacej dokumentácie a potreby kontinuálneho zlepšovania riadenia informačnej bezpečnosti,
g) poskytnutia dostatočných zdrojov na zabezpečenie riadenia informačnej bezpečnosti.

4. Ciele informačnej bezpečnosti

Cieľom bezpečnostnej stratégie CAMOSR je vytvoriť také smerovanie riadenia informačnej bezpečnosti, aby vzniklo a bolo spravované bezpečné a dôveryhodné prostredie, ktoré zaručí, že kvalifikované dôveryhodné služby CAMOSR budú poskytované v požadovanom čase a kvalite a v súlade s platnou legislatívou.

Za hlavné ciele informačnej bezpečnosti CAMOSR považuje vedenie prevádzkovateľa CAMOSR:

a) poskytovanie kvalifikovaných dôveryhodných služieb CAMOSR v súlade so základnými princípmi a zásadami informačnej bezpečnosti,
b) zabezpečenie kontinuity činnosti poskytovania kvalifikovaných dôveryhodných služieb CAMOSR,
c) zabezpečenie riešenia bezpečnostných incidentov súvisiacich s poskytovaním kvalifikovaných dôveryhodných služieb CAMOSR,
d) zaistenie vysokej spoľahlivosti činnosti CAMOSR so zabezpečením dôvernosti, integrity a dostupnosti spracovávaných informácií a osobných údajov,
e) udržanie reputácie a zachovanie dobrého mena CAMOSR v očiach verejnosti,
f) zabezpečenie procesov, vedomostí a technológií CAMOSR,
g) splnenie požiadaviek vyplývajúcich z legislatívy, vnútorných predpisov a štandardov týkajúcich sa poskytovania kvalifikovaných dôveryhodných služieb.

Pre naplnenie hlavných cieľov informačnej bezpečnosti sú navrhnuté operatívne (krátkodobé) ciele informačnej bezpečnosti. Každý operatívny cieľ informačnej bezpečnosti má stanovenú metriku, pomocou ktorej sa vyhodnocuje úspešnosť plnenia cieľa a zamestnanca zodpovedného za jej plnenie. Operatívne ciele informačnej bezpečnosti sú prevádzkovateľom CAMOSR prehodnotené raz za rok a prijaté prípadne nové operatívne ciele informačnej bezpečnosti na nasledujúce obdobie.

V nasledujúcej tabuľke sú uvedené základné operatívne ciele informačnej bezpečnosti CAMOSR.

Tabuľka č. 1: Základné operatívne ciele informačnej bezpečnosti

ID	Cieľ	Metrika (KPI)	Zodpovednosť
1	Vykonanie analýzy rizík raz ročne.	Bola za posledných 12 mesiacov vykonaná analýza rizík?	Hlavný bezpečnostný manažér
2	Vykonanie interného auditu CAMOSR raz ročne.	Bol za posledných 12 mesiacov vykonaný interný audit CAMOSR?	Interný audítor
3	Plnenie úloh vyplývajúcich z vyšetrovania bezpečnostných incidentov.	Počet úloh vyplývajúcich z vyšetrovania bezpečnostných incidentov po termíne.	Hlavný bezpečnostný manažér
4	Minimalizácia zistených nedostatkov z externého auditu CAMOSR.	Počet zistených nedostatkov z externého auditu CAMOSR.	Hlavný bezpečnostný manažér
5	Zabezpečenie vykonania bezpečnostného testovania CAMOSR raz ročne.	Počet zistených závažných bezpečnostných chýb IS CAMOSR.	PMA

ID	Cieľ	Metrika (KPI)	Zodpovednosť
6	Zabezpečenie pravidelného vzdelávania zamestnancov CAMOSR v oblasti informačnej bezpečnosti.	% zamestnancov, ktorí prešli školením.	Hlavný bezpečnostný manažér
7	Zabezpečenie poskytovania kvalifikovaných dôveryhodných služieb	Počet dní v roku kedy neboli poskytované kvalifikované dôveryhodné služby CAMOSR	Administrátor
8	Zabezpečenie riešenia bezpečnostných incidentov súvisiacich s poskytovaním kvalifikovaných dôveryhodných služieb CAMOSR	Počet nových incidentov za kalendárny rok	Hlavný bezpečnostný manažér

5. Vyhodnocovanie cieľov informačnej bezpečnosti

Prevádzkovateľ CAMOSR vyhodnocuje plnenie operatívnych cieľov informačnej bezpečnosti vyhodnotením príslušných metrík v spolupráci so zodpovednými zamestnancami za dané operatívne ciele.

Interný audit nezávisle posudzuje plnenie dosahovania operatívnych cieľov informačnej bezpečnosti raz za rok v rámci auditu CAMOSR.

6. Úlohy prevádzkovateľa CAMOSR v riadení informačnej bezpečnosti

Ministerstvo obrany Slovenskej republiky prevádzkuje CAMOSR 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 (ďalej len zákon o dôveryhodných službách) a Nariadením 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.

Vedenie CAMOSR považuje zabezpečenie informačnej bezpečnosti a spoľahlivosti svojho informačného systému CAMOSR za svoju základnú úlohu, bez plnenia ktorej by certifikačná autorita nemohla plniť úlohy dané zákonom a to so zameraním na poskytovanie kvalifikovaných dôveryhodných služieb a ochranu osobných údajov.

Nadväzne na tento dokument je vypracovaná ďalšia dokumentácia pre jednotlivé oblasti riadenia informačnej bezpečnosti, popisujúca konkrétne pravidlá, postupy, zodpovednosti a činnosti zodpovedných zamestnancov ako aj opatrenia potrebné na splnenie požiadaviek, definovaných touto bezpečnostnou stratégiou.

Vzhľadom na to, že Ministerstvo obrany Slovenskej republiky prevádzkuje certifikačnú autoritu v súlade so zákonom o dôveryhodných službách, je bezpečnostná stratégia vypracovaná aj s ohľadom na požiadavky tohto zákona ako aj zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len zákon o ochrane osobných údajov) a 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).

7. Zodpovednosti v riadení informačnej bezpečnosti

Vedenie CAMOSR sa plne stotožňuje so základnými cieľmi informačnej bezpečnosti a zaväzuje sa vytvárať na ich dosiahnutie potrebné personálne, organizačné, právne, materiálne, technické a finančné podmienky a zabezpečovať informačnú bezpečnosť ako neoddeliteľnú súčasť všetkých riadiacich procesov CAMOSR.

Vedenie CAMOSR zodpovedá za ochranu osobných údajov spracovávaných v informačnom systéme CAMOSR v súčinnosti so zodpovednou osobou za ochranu osobných údajov a v súlade s požiadavkami zákona o ochrane osobných údajov.

Riadenie informačnej bezpečnosti CAMOSR je zabezpečované bezpečnostnými rolami definovanými v dokumente Bezpečnostná politika CAMOSR.

Povinnosti jednotlivých rolí riadenia informačnej bezpečnosti sú uvedené v dokumente Pravidlá na výkon certifikačných činností CAMOSR.

8. Základný rámec riadenia aktív

Riadenie aktív informačného systému CAMOSR je základom pre zabezpečenie informačnej bezpečnosti prevádzkovaných kvalifikovaných dôveryhodných služieb CAMOSR.

Základný rámec riadenia aktív je uvedený v dokumente Bezpečnostná politika CAMOSR.

9. Základný rámec riadenia rizík

Riadenie rizík informačného systému CAMOSR je základom pre zabezpečenie informačnej bezpečnosti prevádzkovaných kvalifikovaných dôveryhodných služieb CAMOSR.

Základný rámec riadenia rizík je uvedený v dokumente Bezpečnostná politika CAMOSR.

10. Audit CAMOSR a kontrolná činnosť

Interný audit CAMOSR a jednotlivých LRA vykonáva interný audítor, ktorý musí byť oprávnenou osobou na vykonávanie bezpečnostných auditov informačných systémov.

Podrobný popis auditu CAMOSR je uvedený v dokumente Certifikačný poriadok CAMOSR kapitola 4.7 Audit bezpečnosti a v dokumente Pravidlá na výkon certifikačných činností CAMOSR kapitola 4.5 Audit bezpečnosti.

Kontrolná činnosť v rámci poskytovania kvalifikovaných dôveryhodných služieb CAMOSR je uvedená v dokumente Pravidlá informačnej bezpečnosti CAMOSR.

11. Riadenie zmien

11.1. Aktualizácia bezpečnostnej stratégie

Bezpečnostná stratégia CAMOSR predstavuje strategický 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.

11.2. 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 stratégii je dlhodobá, záväzná a platná po schválení.

11.3. 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.

Garantom tohto dokumentu je vedúci CAMOSR.

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

12. Odkazy

Ako legislatívne východiská slúži:

- 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
- 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 stratégie:

- 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).