VOJENSKÝ ÚTVAR 9066
TRENČÍN

Č.: 6.spojp-EL 7/11-1-19/2023

Trenčín, 18. apríl 2023
Výtlačok jediný.
Počet listov: 22

Schvaľujem: _____

Pravidlá informačnej bezpečnosti CAMOSR

„Verejný dokument“

Spracovateľ: Sektor informačnej bezpečnosti / Centrum správy IB / 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.	16.11.2022	Finálna verzia dokumentu

Obsah

1. Zoznam obrázkov a tabuliek

1.1. Obrázky

Dokument neobsahuje obrázky

1.2. Tabuľky

Dokument neobsahuje tabuľky

2. Pojmy a skratky

2.1. Pojmy

Aktívum – čokoľvek, čo má pre CAMOSR hodnotu a je to potrebné chrániť. Aktíva CAMOSR 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.

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 informačnú bezpečnosť CAMOSR, 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 byť 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.

Entita – prvok vyznačujúci sa vlastnosťami, ktoré umožňujú jeho jednoznačné odlíšenie od ostatných podobných prvkov nejakej množiny (napr. entitami CAMOSR sú ľudia, systémy, zariadenia, informácie, procesy a pod.).

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 CAMOSR ako celku. Výsledkom hrozby môže byť 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 CAMOSR.

Informačná technológia – prostriedok alebo postup, ktorý slúži na spracúvanie údajov alebo informácií v elektronickej podobe, najmä informačný systém, infraštruktúra, informačná činnosť a elektronické služby.

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

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

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.

Zamestnanec CAMOSR – civilný zamestnanec alebo profesionálny vojak podieľajúci sa na prevádzke CAMOSR.

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 kvalifikované dôveryhodné služby pre MOSR
DRKIS	–	Dozorný riadenia komunikačných a informačných systémov
FW	–	Bezpečnostná brána (Firewall)
IDS	–	Systém detekcie prienikov (Intrusion Detection System)
IT	–	Informačné technológie

LAN	–	Lokálna počítačová sieť
MOSR	–	Ministerstvo obrany Slovenskej republiky
PMA	–	Autorita pre správu politík (Policy Management Authority)
SR	–	Slovenská republika
SW	–	Softvér
WAN	–	Počítačová a komunikačná sieť združujúca viac LAN
WWW	–	World Wide Web, graficky orientované spracovávanie informácií pomocou www stránok
6.spojp	–	Základňa stacionárnych komunikačných a informačných služieb

3. Identifikácia dokumentu a rozsah platnosti

Pravidlá informačnej bezpečnosti CAMOSR podrobne popisujú jednotlivé oblasti riadenia informačnej bezpečnosti certifikačnej autority Ministerstva obrany Slovenskej republiky (ďalej len CAMOSR) Olbrachtova 5, 911 01 Trenčín v súlade s požiadavkami normy STN EN ISO/IEC 27001 a STN EN ISO/IEC 27002.

Pravidlá informačnej bezpečnosti CAMOSR sa vzťahujú na všetkých zamestnancov podieľajúcich sa na poskytovaní kvalifikovaných dôveryhodných služieb CAMOSR v súlade s platnou legislatívou a zamestnancov rezortu ministerstva obrany využívajúcich kvalifikované dôveryhodné služby CAMOSR.

4. Politiky informačnej bezpečnosti

Prevádzkovateľ CAMOSR vypracoval a schválil tieto základné politiky riadenia informačnej bezpečnosti:

- Bezpečnostná stratégia CAMOSR,
- Bezpečnostná politika CAMOSR.

Podrobný popis jednotlivých opatrení normy STN EN ISO/IEC 27001 sa nachádza v tomto dokumente a prevádzkovej dokumentácii CAMOSR.

5. Riadenie informačnej bezpečnosti

Riadenie informačnej bezpečnosti CAMOSR zabezpečuje prevádzkovateľ CAMOSR.

Cieľom riadenia informačnej bezpečnosti je primárne:

- špecifikovať jasné zásady informačnej bezpečnosti CAMOSR,
- zabrániť porušovaniu platných legislatívnych noriem,
- zabrániť, prípadne minimalizovať možnosť finančnej a majetkovej ujmy,
- zabezpečiť dôveryhodnosť poskytovaných kvalifikovaných dôveryhodných služieb CAMOSR,
- zabrániť neautorizovanému prístupu k aktívam CAMOSR,
- umožniť vykonávanie kontroly prístupu k aktívam,
- zabezpečiť dostupnosť informácií pre používateľov a tretie strany,
- zabrániť neautorizovanej modifikácii dát a iných aktív,
- možnosť overenia pôvodu informácií,
- identifikovať možné hrozby pôsobiace na aktíva,
- navrhnúť bezpečnostné opatrenia na ochranu aktív,
- špecifikovať bezpečnostné nástroje na zmenšenie rizika,
- definovať bezpečnostné postupy a nástroje na obnovenie činností po bezpečnostnom incidente,
- definovať bezpečnostné roly spolu s ich zodpovednosťami a právomocami,
- definovať základné pravidlá rozvoja a výberu nových používaných prostriedkov a technológií,
- umožniť sledovanie a hodnotenie stavu informačnej bezpečnosti.

CAMOSR má definované tieto bezpečnostné roly:

- autorita pre správu politík – PMA,
- hlavný bezpečnostný manažér,
- bezpečnostný manažér IDS,
- bezpečnostný manažér FW,
- interný audítor,
- administrátor certifikačnej autority,
- systémový administrátor,
- operátor certifikačnej autority,
- operátor registračnej autority.

5.1. Zodpovednosti a povinnosti bezpečnostných rolí

5.1.1. Autorita pre správu politík - PMA

Interné údaje prevádzkovateľa CAMOSR.

5.1.2. Hlavný bezpečnostný manažér

Interné údaje prevádzkovateľa CAMOSR.

5.1.3. Bezpečnostný manažér IDS

Interné údaje prevádzkovateľa CAMOSR.

5.1.4. Bezpečnostný manažér FW

Interné údaje prevádzkovateľa CAMOSR.

5.1.5. Interný audítor

Interné údaje prevádzkovateľa CAMOSR.

5.1.6. Administrátor certifikačnej autority

Interné údaje prevádzkovateľa CAMOSR.

5.1.7. Systémový administrátor certifikačnej autority

Interné údaje prevádzkovateľa CAMOSR.

5.1.8. Operátor certifikačnej autority

Interné údaje prevádzkovateľa CAMOSR.

5.1.9. Operátor registračnej autority

Interné údaje prevádzkovateľa CAMOSR.

5.2. Oddelenie právomoci

CAMOSR musí byť zabezpečená proti tomu, aby bola jedna osoba schopná kompromitovať systém (single-handedly) špecifikovaním úrovní (rolí) a zodpovedností medzi viaceré osoby.

Je možné, aby niektoré osoby mali viaceré úrovne (roly), ale je potrebné definovať nezlučiteľnosť úrovní (rolí), typicky musia byť oddelené úrovne (roly):

- implementujúce politiku,
- vykonávajúce registráciu,
- vykonávajúce audit.

Toto rozdelenie je postačujúce na zabezpečenie CAMOSR proti kompromitácii.

5.3. Kontakty s orgánmi moci

CAMOSR pri komunikácii so štátnymi orgánmi zastupuje Vojenské spravodajstvo.

5.4. Informačná bezpečnosť v projektovom riadení

Projektové riadenie je v kompetencii organizačného útvaru MOSR zodpovedného za riadenie modernizácie.

6. Personálna bezpečnosť

Personálna bezpečnosť je súčasťou širšej personálnej politiky a jej cieľom je pokrytie hrozieb predstavovaných zamestnancami, dodávateľmi, žiadateľmi, neskúsenými používateľmi, hackermi a špiónmi a pod.. Cieľom personálnej bezpečnosti je tiež ochrana vlastných zamestnancov.

6.1. Uchádzači o zamestnanie a pracovné zmluvy

Každý uchádzač o zamestnanie musí byť pred uzavretím pracovného pomeru preverený s ohľadom na charakter funkcie o ktorú sa uchádza.

Dôraz je potrebné venovať na kontrolu úplnosti a pravdivosti uchádzačom predložených dokumentov a materiálov (doklady, vzdelanie, trestnú bezúhonnosť, atď.)

V prípade, že uchádzač bude pracovať s prostriedkami informačných technológií, je potrebné, aby boli jeho vedomosti overené z hľadiska požadovanej kvalifikácie na danú funkciu, prípadne aj na základe jeho referencií.

Od zamestnancov je v pracovnej zmluve vyžadovaná dohoda o mlčanlivosti o citlivých skutočnostiach, s ktorými sa oboznámi počas výkonu funkcie a to aj po skončení pracovného pomeru.

Je vypracovaný mechanizmus, ktorý zabezpečí deaktivovanie prístupových práv k aktívam CAMOSR, vrátane prístupových hesiel do CAMOSR, odovzdávania kľúčov, zmenu prístupových kódov k poplašnému systému narušenia a podobne.

6.2. Bezpečnostné povedomie a školenia

Prevádzkovateľ CAMOSR zodpovedá za zvyšovanie bezpečnostného povedomia svojich zamestnancov. Každý zamestnanec si musí byť vedomý bezpečnostných hrozieb a musí vedieť správne používať zodpovedajúce prostriedky na spracovávanie informácií tak, aby boli minimalizované bezpečnostné riziká. Súčasťou bezpečnostného povedomia zamestnancov je aj ich povinnosť upozorňovať zodpovedných zamestnancov na zistené bezpečnostné riziká a bezpečnostné udalosti.

Prevádzkovateľ CAMOSR zabezpečí svojim zamestnancom všetky potrebné školenia k bezpečnostnej politike, bezpečnostným postupom organizácie, prípadne školenia, ktoré sú vyžadované príslušnými zákonmi. Súčasťou týchto školení musia byť aj nácviky zvládnutia krízových situácií, realizácie havarijných plánov a plánov obnovy.

Zamestnanci musia byť vždy informovaní o platných bezpečnostných pravidlách a postupoch organizácie preukázateľným spôsobom.

Za preukázateľný spôsob o vykonaní školenia je považovaný písomný zápis, v ktorom účastníci svojím podpisom potvrdia absolvovanie školenia, porozumenie jeho obsahu a svoj záväzok, že sa budú v jeho zmysle správať.

6.2.1. Školenia pre správcov systému

Interné údaje prevádzkovateľa CAMOSR.

6.2.2. Školenia pre používateľov systému (zamestnanci CAMOSR)

Interné údaje prevádzkovateľa CAMOSR.

6.2.3. Nácviky opatrení v prípadoch narušenia systému

Interné údaje prevádzkovateľa CAMOSR.

6.3. Bezpečnosť prístupu tretích strán

Ak existuje možnosť, že tretie strany sa môžu oboznámiť s neverejnými informáciami CAMOSR, musí byť takýto prístup zmluvne ošetrený.

Vyplývajúce riziká musia byť identifikované ešte pred umožnením takéhoto prístupu a musia byť zodpovedajúco zmluvne ošetrené. V zmluve musí byť explicitne ošetrený záväzok o mlčanlivosti ako aj o právnej zodpovednosti v prípade porušenia mlčanlivosti.

Špeciálna pozornosť musí byť venovaná kontraktom, pri ktorých sa tretia strana oboznamuje s citlivými informáciami.

7. Riadenie aktív

Cieľom riadenia aktív je:

- identifikovať aktíva,
- rozdeliť ich podľa dôležitosti a citlivosti,
- vymedziť úroveň ich ochrany.

7.1. Identifikácia a klasifikácia aktív

Identifikácia a evidencia aktív je nutná k zaisteniu bezpečnosti ale aj k iným významným účelom ako je napr. ochrana zdravia, poistenia apod. Za aktívum zodpovedá jeho vlastník, ktorý stanovuje klasifikáciu a určuje kategóriu aktíva. Pri identifikácii jednotlivých aktív je potrebné vziať do úvahy nasledovné spektrum aktív:

- procesy, služby,
- informačné aktíva,
- programové alebo aplikačné aktíva (softvér),
- fyzické aktíva (hardvér),
- komunikačné siete,
- lokality,
- personál,

Ďalším faktorom na stanovenie klasifikácie aktív je obchodné tajomstvo (v zmysle Obchodného zákonníka) a informácie od tretích strán, s ktorými zamestnanci CAMOSR pracujú pri realizácii konkrétnych projektov.

Základné delenie informácií CAMOSR je rozdelené do troch kategórií:

- verejné – informácie verejne prístupné – cenník, certifikačná politika, vzory formulárov,
- interné – informácie určené pre interné použitie v rámci CAMOSR – smernice, pracovné postupy,
- citlivé – informácie, určené iba pre úzky okruh zamestnancov – osobné údaje, analýza rizík, zmluvy

Za zostavenie klasifikácie aktív podľa stupňa ich citlivosti zodpovedá vedúci CAMOSR. Klasifikácia musí byť pravidelne, minimálne jeden krát ročne, podrobená internému auditu, nakoľko v priebehu času môže byť zmenená citlivosť jednotlivých aktív.

7.2. Vrátenie aktív

Ukončením pracovného pomeru alebo iného obdobného pracovného vzťahu zamestnancov CAMOSR a zamestnancov tretích strán sa zdokumentovaným spôsobom vracajú späť všetky zverené aktíva.

CAMOSR získava, spracováva, vytvára a uchováva informácie reprezentované dokumentmi v papierovej aj elektronickej forme.

7.3. Bezpečnosť dokumentov

Na zabezpečenie adekvátnej ochrany informácií a dokumentov sú v závislosti od klasifikácie dokumentu definované schválené spôsoby manipulácie.

Fyzická ochrana nosičov informácie musí podliehať primeraným bezpečnostným pravidlám CAMOSR.

7.3.1. Označovanie

Verejné informácie sa neoznačujú.

Iné ako verejné informácie sa označujú nasledovným spôsobom:

- tlačené alebo písomné materiály musia mať viditeľne vyznačenú ich klasifikáciu v päte každej strany hodnotou Interné údaje – CAMOSR alebo Citlivé údaje – CAMOSR,
- materiály v elektronickej forme sa označujú v päte každej strany hodnotou Interné údaje – CAMOSR alebo Citlivé údaje – CAMOSR,
- informačné médiá (disketa, CD-ROM, DAT páska a podobne) majú klasifikáciu vyznačenú hodnotou Interné údaje – CAMOSR alebo Citlivé údaje – CAMOSR v rámci etikety na médiu aj na obale média.

Materiál musí byť označený ihneď po jeho vzniku. Za jeho správne označenie a príslušnú klasifikáciu je zodpovedná osoba, ktorá materiál vytvorila. V prípade, že materiál pochádza z externých zdrojov, je za jeho označenie a klasifikáciu zodpovedná osoba, ktorá ho prevzala.

V prípade, že dôjde k zmene v klasifikácii materiálu, musí byť príslušná zmena na ňom jednoznačne vyznačená spolu s dátumom zmeny a s podpisom osoby, ktorá zmenu vykonala.

7.3.2. Výmena informácií

Za výmenu informácií sa považuje výmena na ľubovoľnom nosiči (papier, pamäťové médium) ako aj výmena v rámci elektronickej komunikácie (email, Internet).

Pri výmene informácií sa rozlišuje výmena v rámci interného obehu informácií a externá výmena, kedy jeden z účastníkov nie je zamestnancom CAMOSR.

Externá aj interná výmena informácií musí byť zabezpečená tak, aby bola zabezpečená dostatočná ochrana informácií a aby nemohlo dôjsť k ich zneužitiu.

Za dostatočné zabezpečenie v rámci elektronickej komunikácie alebo pri výmene na pamäťovom médiu je považované šifrovanie (PGP, S/MIME, SSL, TLS).

Za dostatočné zabezpečenie pri výmene papierových dokumentov je považované osobné odovzdanie.

Za nedostatočne zabezpečené sa považuje najmä telefonická a faxová výmena, ako aj výmena nešifrovaným emailom.

Externá výmena citlivých informácií je možná iba so súhlasom vedúceho CAMOSR.

7.3.3. Archivácia a likvidácia

Archivácia materiálov (na papierových alebo elektronických nosičoch, ako aj dát v informačných systémoch) musí byť vykonávaná tak, aby bola zabezpečená zodpovedajúca ochrana archivovaných materiálov pred neoprávneným prístupom a bolo tak zabránené ich zneužitiu, aby bola zabezpečená dostupnosť archivovaných materiálov a aby bolo zabránené modifikácii archivovaných materiálov.

Ak pominie dôvod na spracovanie alebo archivovanie informácií, alebo je nutné z iných dôvodov ukončiť spracovávanie informácií je potrebné vykonať likvidáciu príslušných informácií.

Likvidáciu informácií je potrebné vykonať tak, aby ich nebolo možné bežnými prostriedkami obnoviť a aby boli dodržané všetky požiadavky príslušných zákonov a vyhlášok.

Pred likvidáciou je potrebné vždy vziať do úvahy prípadnú archivačnú lehotu, ktorú vyžaduje príslušná legislatívna norma.

Citlivé a interné údaje CAMOSR musia byť z médií bezpečným spôsobom vymazané predtým, než sa médium použije na iný účel. Ak je médium obsahujúce citlivé alebo interné údaje nefunkčné, musí sa zničiť kvalifikovaným spôsobom tak, aby z neho nebolo možné vyčítať údaje.

7.4. Uloženie pamäťových médií

Pamäťové médiá musia byť ukladané v súlade s odporúčaniami výrobcu na ich skladovanie. Pamäťové médiá obsahujúce citlivé informácie musia byť uložené v bezpečných priestoroch, alebo musia byť chránené šifrovaním.

Špecifické nosiče, hlavne tie, ktoré sú určené pre dlhodobú archiváciu musia byť uložené minimálne v dvoch, od seba dostatočne vzdialených lokalitách v zabezpečenom priestore.

8. Riadenie prístupu

8.1. Identifikácia a autentizácia

CAMOSR obsahuje viaceré podsystémy so samostatne riadeným prístupom.

Pre identifikáciu a autentifikáciu administrátorov, operátorov a audítorov je potrebné prihlasovacie meno a heslo (systémový prístup do serverov - meno, heslo resp. certifikát).

Pre identifikáciu a autentifikáciu oprávnených používateľov podsystému CAMOSR (lokálna registračná autorita) je potrebná dvojfaktorová metóda autentifikácie – autentifikácia používateľa s použitím autentifikačného predmetu (čipovej karty/tokenu s certifikátom) a prístupovej PIN frázy ku karte/tokenu.

8.2. Riadenie prístupu

Prístup k aktívam musí byť riadený na základe prevádzkových a bezpečnostných požiadaviek. Uplatňuje sa princíp, že používateľ má tzv. minimálny, nevyhnutne nutný prístup k informáciám.

Bezpečnostný manažér vedie záznamy o aktuálnych prístupových právach zamestnancov podieľajúcich sa na poskytovaní kvalifikovaných služieb. Tento záznam musí byť revidovaný vlastníkmi najmenej raz za rok. Prevádzkovateľ CAMOSR má zavedený proces riadenia prístupových práv do CAMOSR.

8.2.1. Úrovne oprávnení používateľov

Interné údaje prevádzkovateľa CAMOSR.

8.2.2. Práva a povinnosti oprávnených osôb

Interné údaje prevádzkovateľa CAMOSR.

8.2.3. Spôsob identifikácie a autentizácie používateľov

Interné údaje prevádzkovateľa CAMOSR.

8.2.4. Pravidlá pre vytváranie používateľských účtov

Interné údaje prevádzkovateľa CAMOSR.

8.2.5. Pravidlá pre vytváranie a bezpečné používanie používateľských hesiel

Interné údaje prevádzkovateľa CAMOSR.

9. Fyzická bezpečnosť a objektová bezpečnosť

Cieľom fyzickej a objektovej bezpečnosti je zabrániť náhodnému ako aj cielenému neautorizovanému prístupu, poškodeniu, alebo narušeniu aktív v priestoroch CAMOSR Príslušná ochrana musí zodpovedať zisteným rizikám.

Aktíva musia byť umiestnené v bezpečných zónach a chránené bezpečnostným perimetrom a zodpovedajúcimi bezpečnostnými systémami. Všetky prostriedky v bezpečnostných zónach musia byť chránené proti neautorizovanému prístupu, poškodeniu a narušeniu. Celková ochrana musí zodpovedať zisteným rizikám.

Pravidlá pre ochranu bezpečnostných zón sú detailne popísané v dokumente Bezpečnostná dokumentácia fyzickej a objektovej bezpečnosti 6.spojp US1-24-4/2020-V74, ktorý obsahuje podrobné pravidlá pre fyzickú a objektovú bezpečnosť.

Pre všetkých zamestnancov platí zásada prázdneho stolu a umiestnenia zobrazovacích zariadení (monitor) s cieľom znížiť riziko neoprávneného prístupu, straty alebo poškodenia aktív.

9.1. Umiestnenie pracovísk a zariadení

Interné údaje prevádzkovateľa CAMOSR.

9.2. Ochrana a bezpečnosť budov

Interné údaje prevádzkovateľa CAMOSR.

10. Riadenie bezpečnosti prevádzky

Riadenie bezpečnosti prevádzky CAMOSR je jedným zo základných prvkov riadenia informačnej bezpečnosti.

10.1. Prevádzkové postupy a zodpovednosť

Prevádzka CAMOSR je zabezpečená prostredníctvom definovaných rolí, ktorých zodpovednosti sú bližšie špecifikované v kapitole 5.1.

Riadenie zmien CAMOSR je realizované zdokumentovaným procesom aj s podporou dodávateľa na základe požiadavky prevádzkovateľa CAMOSR.

Testovacie a produkčné prostredie CAMOSR sú vzájomne oddelené, čím sa zníži riziko neautorizovaného prístupu alebo zmien v produkčnom prostredí.

10.2. Infraštruktúra CAMOSR

Popis infraštruktúry CAMOSR sa nachádza v samostatnom dokumente Hardvérové a softvérové produkty certifikačnej autority MOSR.

10.3. Antivírusové programové vybavenie

Všetky pracovné stanice a prenosné počítače musia používať schválené antivírusové programové vybavenie. Antivírusový softvér musí byť pravidelne aktualizovaný a všetky vymeniteľné médiá musia byť pred použitím skontrolované na výskyt vírusovej infekcie.

10.4. Zálohovanie

Zálohovanie informačných aktív CAMOSR sa realizuje v súlade s dokumentom Metodika zálohovania informačných aktív CAMOSR.

10.5. Zaznamenávanie dát a monitorovanie

Cieľom monitorovania CAMOSR je detegovať a dokumentovať neautorizované aktivity.

V CAMOSR musia byť vytvárané auditné záznamy obsahujúce identifikáciu používateľa, dátum a čas prihlásenia a odhlásenia, identifikáciu miesta, odkiaľ sa používateľ prihlasoval (pokiaľ je to možné) a záznamy o prístupe (úspešnom aj neúspešnom) a operáciách s dátami a inými zdrojmi systému.

Na úrovni operačného systému musia byť vytvárané záznamy týkajúce sa neoprávnených prístupov, operácií vykonávanými privilegovanými používateľmi a systémové volania a chyby.

Pre presnosť auditných záznamov je potrebné zabezpečiť časovú synchronizáciu sledovaných systémov.

Všetky auditné záznamy musia byť sledované, pravidelne kontrolované a analyzované.

10.6. Riadenie zraniteľností informačných technológií

Riadenie zraniteľností CAMOSR je procesom, ktorý minimalizuje riziká súvisiace s prevádzkou informačných technológií.

Riadenie zraniteľností CAMOSR sa rozdeľuje do 3 fáz:

- detekcia a hlásenie,
- posúdenie a rozhodnutie,
- reakcia.

10.6.1. Detekcia a hlásenie

Interné údaje prevádzkovateľa CAMOSR.

10.6.2. Posúdenie a rozhodnutie

Interné údaje prevádzkovateľa CAMOSR.

10.6.3. Reakcia

Interné údaje prevádzkovateľa CAMOSR.

10.7. Bezpečnosť pracovných staníc

Všetky pracovné stanice môžu byť používané výlučne na pracovné účely. Na pracovných staniciach môže byť nainštalovaný iba schválený softvér, nevyhnutne potrebný pre prácu zamestnanca. Všetky pracovné stanice musia mať aktivovaný šetrič obrazovky s heslom. Programové vybavenie musí byť pravidelne aktualizované.

10.8. Bezpečnosť prenosných počítačov

Všetky prenosné počítače môžu byť používané výlučne na pracovné účely. Na prenosných počítačoch môže byť nainštalovaný iba schválený softvér, nevyhnutne potrebný pre prácu zamestnanca. Všetky prenosné počítače musia mať aktivovaný šetrič obrazovky s heslom. Ak sú na prenosnom počítači uložené citlivé alebo interné údaje, musia byť tieto chránené šifrovaním. Programové vybavenie prenosných počítačov je pravidelne aktualizované.

11. Riadenie komunikačnej bezpečnosti

CAMOSR predstavuje centralizovaný informačný systém z hľadiska umiestnenia údajov a distribuovaný z hľadiska rozmiestnenia pracovných staníc.

Komunikácia interných používateľov je realizovaná prostredníctvom LAN, externých prostredníctvom Internetu a WWW rozhrania.

11.1. Sieťová infraštruktúra

Všetci používatelia siete musia dodržiavať pravidlá pripojenia do siete.

Vzdialený prístup do siete je obmedzený a je umožnený len v odôvodnenom a schválenom prípade.

Prístup do siete a prístup k sieťovým zdrojom je povolený výlučne iba autorizovaným osobám.

Nastavenie sieťovej infraštruktúry CAMOSR je realizované v súlade s dokumentom Nastavenia zariadení a sieťovej infraštruktúry CAMOSR.

11.2. Internet

CAMOSR nemá pripojenie do Internetu.

11.3. Šifrovanie/autentifikácia správ

Na zabezpečenie dôvernosti pri prenose dát po sieti Internet alebo RDS je použité šifrovanie. Šifrovanie a elektronický podpis sa využíva aj pri emailovej komunikácii.

12. Riadenie vývoja a údržby

CAMOSR je vyvíjaná dodávateľom v súlade s predmetnými zmluvami.

Údržbu CAMOSR realizujú zodpovední zamestnanci CAMOSR.

Pravidelnú preventívnu kontrolu informačných systémov je potrebné vykonávať minimálne jedenkrát do roka zamestnancami CAMOSR, resp. externou organizáciou podľa zmluvy. O výsledku tejto kontroly je potrebné vypracovať písomný záznam v Prevádzkovej knihe udalostí a uchovávať ju na pracovisku s prístupom len pre oprávnených zamestnancov.

Taktiež je potrebné vykonávať údržbu informačných technológií zamestnancami CAMOSR, resp. externou organizáciou podľa zmluvy.

Servisná činnosť vykonávaná zamestnancami servisných organizácií musí byť organizovaná s ohľadom na bezpečnosť systému. Pri takýchto prácach treba klásť dôraz na:

- preverenie totožnosti a oprávnenia servisných zamestnancov k danej činnosti,
- zaistenie dozoru pri práci servisných zamestnancov,
- spoľahlivé vymazanie chránených informácií zo všetkých pamäťových médií, ku ktorým by mohol mať servisný zamestnanec prístup, resp. ich uloženie mimo dosahu servisných zamestnancov,
- zaistenie spoľahlivého vymazania médií odoslaných k oprave,
- organizáciu ostatných činností, ktoré súvisia s opravami a technickou údržbou a ktoré by mohli nepriaznivo ovplyvniť bezpečnosť systému.

Servisnú podporu vykonávanú externou organizáciou, ktorá vystupuje ako dodávateľ je možné v prostredí CAMOSR vykonávať len na základe uzatvorenej platnej zmluvy. S každou externou organizáciou je potrebné uzavrieť samostatnú zmluvu o výkone servisnej podpory.

13. Riadenie dodávateľských vzťahov

Prevádzkovateľ CAMOSR môže v prípade potreby použiť na niektoré činnosti dodávateľské zdroje. Prevádzkovateľ CAMOSR zabezpečí vhodnú ochranu aktív pri využívaní služieb tretích strán.

13.1. Zmluvné bezpečnostné požiadavky na ochranu aktív

Všetky prístupy tretích strán k aktívam CAMOSR musia byť zmluvne ošetrené alebo musí byť iným spôsobom vykonaná ochrana týchto aktív. Vyplývajúce riziká musia byť ešte pred umožnením takého prístupu identifikované a náležite ošetrené.

Zmluvy by mali z hľadiska informačnej bezpečnosti obsahovať:

- všeobecné pravidla informačnej bezpečnosti,
- ochranu aktív,
- opatrenia umožňujúce ukončenie alebo zmenu zmluvného vzťahu bez bezpečnostného rizika,
- pravidlá na utajenie, nešírenie informácií, neporušenie integrity a dostupnosti aktív,
- špecifikáciu každej sprístupnenej služby a jej úrovne,
- v prípade potreby podmienky vzájomného prechodu, resp. odchodu zamestnanca tretej strany,
- konkrétne zmluvné záväzky,
- zodpovednosti dohodnuté a vyplývajúce s právnych noriem,
- ochranu duševného vlastníctva a autorského práva,
- podmienky, metódy a oblasti prístupu,
- právo monitorovať a povoľovať aktivity používateľa,
- právo auditovať zmluvné povinnosti,
- pravidlá na riešenie havarijných situácií,
- zodpovednosť za prácu a vlastné produkty,
- systém hlásení a komunikácie v oblasti informačnej bezpečnosti,
- pravidlá procesu riadenia zmien,
- pravidlá školení.

14. Riadenie bezpečnostných incidentov

Cieľom riadenia bezpečnostných incidentov je minimalizovať škody spôsobené bezpečnostnými incidentmi a chybami, sledovať, evidovať, predvídať iné incidenty a učiť sa z nich.

Medzi základné povinnosti každého zamestnanca/používateľa CAMOSR patrí:

- Hlásiť bezpečnostné incidenty – hneď ako je zistený bezpečnostný incident, má zamestnanec povinnosť predpísaným postupom o tejto skutočnosti informovať.
- Hlásiť bezpečnostné slabiny – zamestnanec musí v prípade spozorovania zaznamenať zraniteľné miesta alebo hrozby a predpísaným postupom o tejto skutočnosti informovať.
- Hlásiť chybné fungovanie programového vybavenia – o chybnom fungovaní programového vybavenia musí zamestnanec predpísaným postupom informovať.

Bezpečnostné incidenty, slabiny a chybné fungovanie programového vybavenia musia byť analyzované tak, aby bolo možné realizovať preventívne opatrenia pre zabránenie opakovania incidentu. Ďalej musia byť incidenty a chyby kvantifikované pre pravidelné štatistické výkazy hmotných strát.

Za analýzu bezpečnostných incidentov, slabín a chybného fungovania programového vybavenia je zodpovedný hlavný bezpečnostný manažér.

14.1. Metodika riadenia bezpečnostných incidentov

Riadenie bezpečnostných incidentov CAMOSR znamená zabezpečenie riešenia udalostí a incidentov súvisiacich s prevádzkou informačných technológií oznamované primeraným spôsobom, ktorý včas umožní podniknutie potrebných nápravných činností.

Proces riadenia bezpečnostných incidentov CAMOSR sa rozdeľuje do 5 fáz:

- plánovanie a príprava,
- detekcia a hlásenie,
- posúdenie a rozhodnutie,
- reakcia,
- poučenie

14.1.1. Plánovanie a príprava

Interné údaje prevádzkovateľa CAMOSR.

14.1.2. Detekcia a hlásenie

Interné údaje prevádzkovateľa CAMOSR.

14.1.3. Posúdenie a rozhodnutie

Interné údaje prevádzkovateľa CAMOSR.

14.1.4. Reakcia

Interné údaje prevádzkovateľa CAMOSR.

14.1.5. Poučenie

Interné údaje prevádzkovateľa CAMOSR.

15. Riadenie kontinuity činnosti

Cieľom riadenia kontinuity činnosti je zabrániť nežiaducemu prerušeniu činností CAMOSR a chrániť jej kritické procesy pred následkami vážnych chýb a katastrof. Pokiaľ k nežiaducemu prerušeniu príde, je potrebné zabezpečiť rýchlu a bezpečnú obnovu systémov po technickej stránke a definovanie a preverenie procesov obnovy.

15.1. Stratégia plánovania kontinuity činností CAMOSR

Prvou zásadou plánovania kontinuity činností je zavedená a aktívna bezpečnostná kultúra CAMOSR, ktorá umožňuje znížiť zraniteľnosť alebo pravdepodobnosť realizácie scenárov rizík.

Ďalšou zásadou je riadna príprava na možné krízové udalosti. Musí byť vypracovaný havarijný plán, ktorý je základným dokumentom oblasti krízového plánovania. V havarijnom pláne budú obsiahnuté hlavne inicializačné procedúry pre všetky očakávané (možné) krízové udalosti a bude tu zaistená koordinácia postupov a nadväznosť medzi ďalšími plánmi mimoriadnych opatrení.

15.1.1. Predpoklady úspešnej obnovy systému

Interné údaje prevádzkovateľa CAMOSR.

15.1.2. Preventívne opatrenia

Interné údaje prevádzkovateľa CAMOSR.

15.1.3. Účel procesu obnovy systému

15.1.4. Riadenie a zodpovednosť za proces obnovy systému

Interné údaje prevádzkovateľa CAMOSR.

15.1.5. Predmet obnovy systému

Interné údaje prevádzkovateľa CAMOSR.

15.2. Obsah havarijného plánu

Interné údaje prevádzkovateľa CAMOSR.

15.3. Obsah plánu obnovy prevádzky

Interné údaje prevádzkovateľa CAMOSR.

15.4. Uloženie havarijných plánov a plánov obnovy prevádzky

Interné údaje prevádzkovateľa CAMOSR.

15.5. Tvorba a zmeny havarijných plánov a plánov obnovy prevádzky

Interné údaje prevádzkovateľa CAMOSR.

16. Riadenie súladu

Prevádzkovateľ CAMOSR sa v rámci prevádzky CAMOSR riadi týmito legislatívnymi a regulačnými požiadavkami:

- 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. 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) 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),
- zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov,
- 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),
- STN ISO/IEC 27005 - Informačné technológie. Bezpečnostné metódy. Riadenie rizík informačnej bezpečnosti.

17. Kontrolná činnosť

17.1. Spôsob, forma a periodicita výkonu kontrolných činností

17.1.1. Formy kontrolných činností

Zoznam kontrolných činností:

- stála kontrolná činnosť:
  - monitoring CAMOSR,
- periodické kontroly:
  - nastavenia bezpečnostných parametrov zariadení CAMOSR,
  - auditných záznamov,
  - dodržiavania bezpečnostnej politiky správy hesiel,
  - nastavenia prístupových práv používateľov k prvkom a aplikáciám CAMOSR,
  - manipulácie s pamäťovými médiami,
  - zálohovania,
  - revízie záznamov o kontrolách,
- následné kontroly:
  - po odchode alebo preradení zamestnanca predtým pracujúceho s informačným systémom CAMOSR,
  - po zmenách v konfigurácii siete,
  - po nainštalovaní novej verzie operačného systému, aplikácie a databázy spracovávajúcej informácie,
- náhodné kontroly:
  - kontrola niektorej z oblastí určenej v periodických kontrolách.

O zisteniach a výsledkoch z periodických, náhodných a následných kontrol je vypracovaný záznam do Prevádzkovej knihy udalostí. Táto je uložená v bezpečnom úschovnom objekte v miestnosti, ktorá je určená pre ukladanie takýchto materiálov.

17.1.2. Stála kontrolná činnosť

Interné údaje prevádzkovateľa CAMOSR.

17.1.3. Periodické kontroly

Interné údaje prevádzkovateľa CAMOSR.

17.1.4. Následné kontroly

Interné údaje prevádzkovateľa CAMOSR.

17.1.5. Náhodné kontroly

Interné údaje prevádzkovateľa CAMOSR.

18. Riadenie rizík

Účelom riadenia rizík je vymedziť základné pravidlá pre riadenie rizík týkajúcich sa informačnej bezpečnosti CAMOSR.

Cieľom riadenia rizík je identifikácia a ohodnotenie aktív, hrozieb a zraniteľností, výpočet a ohodnotenie rizika, rozhodnutie o správe rizika s následným výberom opatrení a ich realizáciou.

Pri ohodnocovaní rizík CAMOSR bude použitá metodika kvalitatívnej analýzy rizík tak, ako je stanovené normou STN ISO/IEC 27005. Riziká budú stanovené na základe ich možného dopadu a pravdepodobnosti výskytu hrozieb, na činnosť CAMOSR berúc do úvahy aj aspekty zraniteľnosti. Uvedené hodnotenie rizík bude vykonávané raz ročne zodpovedným zamestnancom CAMOSR alebo nezávislou treťou stranou.

Bezpečnostné požiadavky Nariadenia eIDAS týkajúce sa procesu riadenia rizík:

- CAMOSR ako poskytovateľ dôveryhodných služieb je povinná prijať vhodné technické a organizačné opatrenia na riadenie rizík ohrozujúcich bezpečnosť dôveryhodných služieb, ktoré poskytuje. So zreteľom na najnovší technologický vývoj sa uvedenými opatreniami musí zaistiť úroveň bezpečnosti primeranú stupňu rizika.
- CAMOSR je povinná prijať najmä opatrenia na prevenciu a minimalizáciu vplyvu bezpečnostných incidentov a na oznámenie nepriaznivých účinkov všetkých takýchto incidentov zainteresovaným stranám.
- CAMOSR ako poskytovateľ dôveryhodných služieb bez zbytočného odkladu, najneskôr však do 24 hodín odkedy sa dozvedela o akomkoľvek narušení bezpečnosti alebo integrity s významným vplyvom na poskytovanú dôveryhodnú službu alebo osobné údaje uchovávané v rámci nej, oznámi túto skutočnosť zodpovedným orgánom MO SR za informačnú bezpečnosť alebo ochranu osobných údajov.
- Ak môže narušenie bezpečnosti alebo integrity negatívne ovplyvniť fyzickú alebo právnickú osobu, ktorej sa dôveryhodná služba poskytovala, CAMOSR bez zbytočného odkladu oznámi narušenie bezpečnosti alebo integrity aj tejto fyzickej či právnickej osobe.

18.1. Metodika riadenia rizík

Interné údaje prevádzkovateľa CAMOSR.

18.1.1. Charakteristika a opis súčasného stavu prostredia CAMOSR

Interné údaje prevádzkovateľa CAMOSR.

18.1.2. Identifikácia, klasifikácia a ohodnotenie aktív

Interné údaje prevádzkovateľa CAMOSR.

18.1.3. Identifikácia hrozieb

Interné údaje prevádzkovateľa CAMOSR.

18.1.4. Určenie pravdepodobnosti realizácie hrozby

Interné údaje prevádzkovateľa CAMOSR.

18.1.5. Určenie dopadu identifikovaných hrozieb

Interné údaje prevádzkovateľa CAMOSR.

18.1.6. Hodnotenie rizík

Interné údaje prevádzkovateľa CAMOSR.

18.1.7. Návrh bezpečnostných opatrení

Interné údaje prevádzkovateľa CAMOSR.

18.1.8. Určenie zostatkových rizík

Interné údaje prevádzkovateľa CAMOSR.

19. Riadenie zmien

19.1. Aktualizácia dokumentu

Dokument Pravidlá informačnej bezpečnosti CAMOSR predstavuje dokument popisujúci jednotlivé opatrenia riadenia informačnej bezpečnosti.

19.2. 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 tomto dokumente je dlhodobá, záväzná a platná po schválení.

19.3. 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.

19.4. 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.

19.5. Výnimky

Pokiaľ nastane situácia, kedy bude potrebné udeliť výnimku zo zavedených bezpečnostných pravidiel a zásad, ktoré sú dané týmto dokumentom, musí byť táto výnimka odborne posúdená hlavným bezpečnostným manažérom, schválená vedúcim CAMOSR a zodpovedajúcim spôsobom zdokumentovaná.