



REPUBLIKA HRVATSKA

MINISTARSTVO GOSPODARSTVA, RADA I PODUZETNIŠTVA

10000 ZAGREB - Ulica grada Vukovara 78

Klasa: 330-01/04-01/30

Urbroj: 526-01/04-05

NACIONALNI CA ZA REPUBLIKU HRVATSKU (NCARH)

OPĆA PRAVILA O SIGURNOSTI

Verzija 1.0

Datum 22.01.2004.

AUTORSKA PRAVA

Ovaj je dokument u vlasništvu Ministarstva gospodarstva, rada i poduzetništva i FINE i podložan je zaštiti autorskih prava prema zakonima Republike Hrvatske.

KRATICE, REFERENCE I DEFINICIJE

Cjelokupna se dokumentacija referencira na zakone, pravilnike, direktive, standarde i NCARH dokumentaciju, nadalje definirani su standardi za tumačenja pojedinih kratica i pojmova koje se koriste u HR PKI i NCARH dokumentaciji.

Dokument **Kratice, reference i definicije** je u privitku.

PRIMJEDBE I PROMJENE

Mehanizam upravljanja primjedbama

Napisane i potpisane primjedbe na ovaj dokument moraju biti upućene Povjerenstvu za donošenje, uvođenje i provedbu odluka koje se odnose na HR PKI dokumentaciju i procedure.

Obavijest o finalnim promjenama

Povjerenstvo za donošenje, uvođenje i provedbu odluka koje se odnose na HR PKI dokumentaciju i procedure odredit će period za obavijest o finalnim promjenama.

PREGLED PROMJENA

Redni broj	Verzija	Točka	Opis promjene	Datum promjene

OBJAVA

Na temelju odluke o prihvaćanju i objavi dokumenata NCARH-a donijete na sjednici Povjerenstva za donošenje, uvođenje i provedbu odluka koje se odnose na HR PKI dokumentaciju održanoj dana 22.siječnja 2004.godine, Ministarstvo gospodarstva, rada i poduzetništva objavljuje navedene dokumente.

U Zagrebu 15. ožujka 2004.g.


MINISTAR
Branko Vukelić


Sadržaj

1. UVOD	1
1.1. Svrha dokumenta	1
1.2. Politika o sigurnosti (Security Policy)	1
1.2.1. Smisao sigurnosti	1
1.2.2. Upravljanje	2
1.2.3. Arhitektura i planiranje	2
1.2.4. Tehnologija	2
2. PROCEDURE ZA PROVEDBU SIGURNOSTI	2
2.1. Pregled	2
2.1.1. Standardi	3
3. NAČELA POSLOVANJA	3
3.1. Cjelovitost - integritet	3
3.2. Raspoloživost	3
3.3. Ključevi	4
3.3.1. NCARH privatni ključevi	4
3.3.2. Zaštita ključeva	4
3.4. Sigurnosne zone	4
3.4.1. Zone u kojima je potrebna nazočnost dva zaposlenika	4
3.4.2. Kontrole pristupa	5
4. PKI ULOGE I ODGOVORNOSTI	5
4.1. PMA HR PKI	5
4.2. NCARH	5
4.2.1. Voditelj OA NCARH/glavni korisnik	5
4.2.2. Specijalist sigurnosti	5
5. ZAPOSLENICI	6
5.1. PKI povjerljive uloge	6
5.2. Odgovornosti zaposlenika	6
5.3. Privatnost	7
5.4. Školovanje i obuka	7
5.5. Računala i SW u privatnom vlasništvu	7
5.6. Autorska prava na SW	8
5.7. Elektronička pošta	8
5.8. Sankcije	8
6. UPRAVLJANJE NCARH SUSTAVOM	9
6.1. Kontrola upravljanja	9
6.2. Povjerenstvo za kontrolu promjena	9
6.2.1. Kontrola SW	9
6.3. Operacije	10
6.4. Tehnologija	10
7. SIGURNOST INFRASTRUKTURE	11
7.1. Sigurnost mreže	11
7.2. Konfiguracija vatrozida (FIREWALL)	11
8. SIGURNOST PODATAKA	11

NCARH

Opća pravila o sigurnosti

Sadržaj

8.1. Obilježavanje i pohranjivanje osjetljivih medija	11
8.2. Sigurnost medija	11
8.3. Prijenos i pohranjivanje podataka	12
8.4. Prenosiva/Laptop računala	12
8.5. Računalni virusi	12
8.6. Arhiva	12
8.6.1. Tipovi pohranjenih podataka	12
8.6.2. Period arhiviranja	13
9. FIZIČKA ZAŠTITA	13
9.1. Vođenje evidencije pristupa NCARH prostoru	13
9.2. Evidentiranje imovine	13
10. NARUŠAVANJE SIGURNOSTI.....	13
10.1. Unutarnje narušavanje sigurnosti.....	13
10.2. Vanjsko narušavanje sigurnosti	14
10.3. Procedure izvještavanja o unutarnjem ili vanjskom narušavanju sigurnosti.....	14
11. OSIGURANJE KONTINUITETA POSLOVANJA.....	15
11.1. Procjena ranjivosti.....	15
11.2. Plan oporavka u slučaju incidenta (Disaster Recovery Plan).....	15
11.3. Odaziv na kritične incidente	16

1. UVOD

1.1. Svrha dokumenta

Ovaj dokument opisuje na koji način su opća pravila sigurnosti pripremljena, vođena i objavljena. Dokument sadrži dijelove koji se odnose na:

- fizičku sigurnost,
- logičku sigurnost,
- operativnu sigurnost,
- backup i arhiviranje podataka,
- operativno osoblje,
- tajnost informacija,
- detaljne dokumente koji se odnose na opća pravila sigurnosti, uključivo:
 - *plan sigurnosti informatičkog sustava,*
 - *plan fizičke sigurnosti,*
 - *plan oporavka u slučaju incidenta,*
 - *plan backup-a SW i podataka,*
 - *operativni priručnik za NCARH.*

1.2. Politika o sigurnosti (Security Policy)

Politika o sigurnosti je strateški dokument visoke razine i odražava poslovne potrebe Ministarstva gospodarstva, rada i poduzetništva i PMA HR PKI za zaštitom NCARH sustava. Politika sigurnosti sadrži sljedeće:

- zahtjeve PMA HR PKI u provedbi zaštite,
- obvezujuće principe poslovanja u HR PKI, i
- smisao i svrhu sigurnosti u HR PKI.

1.2.1. Smisao sigurnosti

Pristup implementiranju sigurnosti, zasebno fizički koncept, oblikovanje i razvojni proces koji primjenjuje NCARH, temelji se na stavu da se sigurnost izvodi iz tri ključna područja. Oni su ovisni jedan o drugom i zato moraju biti kompatibilni.

Glavni je cilj sigurnosti u NCARH sljedeći:

- spriječiti svaku neautoriziranu akciju koja se pojavi,
 - *otkriti i bilježiti svaku neautoriziranu akciju koja se pojavi,*
- poduzeti akcije koje su potrebne nakon primitka potrebne informacije.

NCARH

Opća pravila o sigurnosti

1.2.2. Upravljanje

Upravljanje se odnosi na kontrole u NCARH koje se odnose na sigurnost i na osobe uključene u održavanje sigurne okoline, njihove zadaće i odgovornost.

1.2.3. Arhitektura i planiranje

Ovo se odnosi na postignutu sigurnost pri izvedbi NCARH prostora, također se odnosi na fizičke barijere koje ograničavaju kretanje na mjesta gdje se nalazi tehnologija, i kontrole pristupa osjetljivim mrežama i infrastrukturi. Arhitektura i planiranje također prepoznaje različite grupe korisnika u okviru NCARH prostora te kako su ti korisnici odijeljeni.

1.2.4. Tehnologija

Tehnološki se element sigurnosti odnosi na opremu koja podržava upravljanje sigurnošću.

2. PROCEDURE ZA PROVEDBU SIGURNOSTI

Procedure za provedbu sigurnosti su skup sigurnosnih postupaka, koji opisuju kako se sredstvima/resursima (uređaji, servisi, informacije i osoblje) upravlja, kako se oni štite i distribuiraju.

Krajnji je cilj dokumenta **Opća pravila o sigurnosti** kreiranje okvira kojim će se osigurati, a kada bude pravilno implementiran, da NCARH postigne najvišu moguću razinu sigurnosti.

Opća se pravila sigurnosti odnose na cijeli sustav na kojem se temelji NCARH, i uvode procedure po kojima se uspješno obavlja izdavanje certifikata i upravljanje njihovim životnim ciklusom.

Navodi su iz ovog dokumenta u skladu s poznatim međunarodnim PKI standardima.

2.1. Pregled

U namjeri da se postigne visoka razina sigurnosti pri provođenju ovoga posla nužno je pokazati da su najviši standardi povjerenja i sigurnosti primijenjeni kod ovih servisa. Ti se standardi očituju postizanjem sljedećeg:

- sigurna fizička okolina,
- pravilnici i procedure,
- tehnologija,
- iskustvo,
- revizija,
- odabir osoblja,
- pravna ekspertiza,
- operacije.

2.1.1. Standardi

Sigurnosna se politika temelji na sljedećim standardima:

- IETF RFC 2196 Site Security Handbook,
- BS 7799-1:1999 Information Security Management. Code of Practice for Information Security Management,
- BS 7799-2:1999 Information Security Management. Specification for Information Security Management Systems.
- ISO 17799
 - *Business Continuity Planning,*
 - *System Access Control,*
 - *System Development and Maintenance,*
 - *Physical and Environmental Security,*
 - *Compliance,*
 - *Personnel Security,*
 - *Security Organization,*
 - *Computer & Operations Management,*
 - *Asset Classification and Control,*
 - *Security Policy.*

3. NAČELA POSLOVANJA

3.1. Cjelovitost - integritet

Zahtjevi za certifikat i informacije u certifikatu u okviru NCARH sustava i X.500 imenika ne mogu se mijenjati, brisati ili dodavati na bilo koji način od strane operativnog osoblja. Ovo je nametnuto kroz upotrebu stroge logične kontrole pristupa, kombinirano s redovitim nadgledanjem NCARH mreže.

Samo autorizirano NCARH i RA operativno osoblje ima dozvolu za dodavanje novih zahtjeva u NCARH sustav. Takvi registracijski zahtjevi ne mogu biti mijenjani, brisani ili dodavani ni na koji način. Nadgledanje na razini aplikacije i podatkovne osnovice bit će uvedeno da bi se kontrolirao pristup tim informacijama. Podatkovna osnovica je zaštićena imenom korisnika i lozinkom.

3.2. Raspoloživost

U skladu sa NCARH politikom davanja usluga, X.500 imenik je dostupan klijentima 24 sata na dan i 7 dana u tjednu. Nemogućnost da klijenti pristupe toj podatkovnoj osnovici znači da se zahtjevi za validaciju certifikata ne mogu procesuirati sve do ponovnog uspostavljanja servisa, odnosno da korisnik neće moći koristiti svoju PKI aplikaciju ili se pouzdati u certifikat. Za NCARH je imperativ održavanje mogućnosti da klijenti mogu neprekidno pristupati tim servisima.

NCARH

Opća pravila o sigurnosti

CRL mora biti dostupna u svako vrijeme radi osiguranja da klijenti imaju mogućnost provjeriti da certifikat s kojim oni rade nije bio opozvan. Nemogućnost da klijent provede tu provjeru može rezultirati provođenjem transakcija koje inače ne bi proveo.

3.3. Ključevi

3.3.1. NCARH privatni ključevi

Tajnost i povjerljivost NCARH privatnih ključeva osigurana je sljedećim mjerama:

- fizička sigurnost na visokoj razini,
- složene logične sigurnosne mjere koje uključuju detekciju upada, višestruke vatrozidove i sistemsko nadgledanje,
- stroge fizičke kontrole pristupa,
- uvođenje pravila o ograničavanju boravka samo jedne osobe u prostorima u kojima se generiraju i pohranjuju ključevi,
- izbor osoblja,
- potpuna organizacija prostora i opreme za oporavak u slučaju nezgode.

3.3.2. Zaštita ključeva

Apsolutni je imperativ zaštita potpisnog ključa i osiguranje da nema nikakvih mogućnosti za kompromitiranje. Plan za oporavak od nezgode, procjena rizika i opasnosti te plan o kontinuitetu (neprekidnosti) rada razvijeni su da bi jamčili sigurnost, raspoloživost i integritet potpisnih ključeva.

Ovi potpisujući ključevi čine temelj PKI sustava povjerenja:

- NCARH ključevi,
- CA ključevi.

3.4. Sigurnosne zone

3.4.1. Zone u kojima je potrebna nazočnost dva zaposlenika

NCARH ima uvedene zone u kojima je potrebna nazočnost najmanje dva zaposlenika, u okviru posebnih područja u višeslojnim sigurnim zonama. To znači da postoje područja u operativnom centru gdje nije dopušteno da osoba bude sama, te je potrebna nazočnost dviju osoba kadgod se ulazi u ta područja.

Zone u kojima je potrebna nazočnost dva zaposlenika uključuju:

- područja u kojima se čuva online kriptografski materijal,
- područja u kojima se čuva offline kriptografski materijal,
- prostorija u kojoj se vrši usluga generiranja ključa, odnosno kada se ona provodi,
- prostor u kojoj je smještena oprema produkcijske mreže.

3.4.2. Kontrole pristupa

Kontrola se pristupa na NCARH računalnu mrežu provodi s lozinkom i/ili certifikatom. Od cjelokupnog se osoblja zahtijeva da se pridržavaju uputa u odnosu na konstrukciju lozinke, upotrebu, vrijeme trajanja i sigurnost, kao što je opisano u priručniku za zaposlenike.

Redovita se kontrola provodi o upotrebi lozinke na sustavu s ciljem da se osigura njihova usklađenost s uputama.

4. PKI ULOGE I ODGOVORNOSTI

4.1. PMA HR PKI

PMA HR PKI je odgovorna za iniciranje promjena i odobravanje Općih pravila sigurnosti, za periodičku reviziju provođenja sigurnosnih procedura te provjeru usklađenosti rada NCARH, RA i LRA s Općim pravilima sigurnosti, CP-om i CPS-om i drugim internim dokumentima.

4.2. NCARH

4.2.1. Voditelj OA NCARH

Voditelj OA NCARH je odgovoran za:

- operativno vođenje OA NCARH,
- pripremu i izdavanje internih priručnika i procedura.

4.2.2. Specijalist sigurnosti

Specijalist sigurnosti je odgovoran za svakodnevno administriranje sigurnosnih postupaka:

- razvoj i implementacija procedura fizičke sigurnosti,
- razvoj i implementacija procedura sigurnosti IT,
- administriranje i nadgledanje procesa promjena,
- nadgledanje revizijskih zapisa,
- promidžbu svijesti o sigurnosti u OA NCARH,
- otkrivanje prekršaja i krivotvorina,
- izobrazbu svih korisnika o pravilima o sigurnosti,
- izvještavanje nadređenog o incidentima.

Cjelokupno je operativno osoblje odgovorno za osiguranje obavljanja poslova u skladu s Općim pravilima o sigurnosti.

5. ZAPOSLENICI

5.1. PKI povjerljive uloge

Kao dio visokog standarda povjerenja i sigurnosti koje implementira PKI, svim zaposlenicima moraju biti provjereni životopisi, te moraju proći financijske i kriminalističke provjere da bi se ustanovila njihova pouzdanost za tu visoku razinu povjerenja.

OA NCARH provodi odgovarajuće istraživanje životopisa osoblja koje radi na povjerljivim korisničkim ulogama (prije zaposlenja te poslije s vremena na vrijeme):

- potvrda o nekažnjavanju,
- provjera ranijih zaposlenja da bi se dobile informacije o godinama rada, profesionalne kvalifikacije, reference i suradnja s kolegama i
- provjera njihove financijske situacije.

5.2. Odgovornosti zaposlenika

Sve osobe moraju potpisati ugovor prije zaposlenja u OA NCARH.

Sve osobe moraju pročitati i potpisati pristanak da su spremne pridržavati se Priručnika za zaposlenike.

Svi su zaposlenici odgovorni za korištenje računalnih resursa, za svaku upotrebu svojih prijava na sustav (logon) te moraju čuvati i ne otkrivati svoje lozinke da bi zaštitili NCARH računalne resurse.

Osobe koje koriste wan servise kao Internet, preko NCARH infrastrukture, moraju poštivati pravila koja su detaljno opisana u Priručniku za zaposlenike.

Zaposlenici neće pokušati pristupiti NCARH resursima za koju nemaju autorizaciju.

Zaposlenici su odgovorni za:

- pridržavanje procedura, primjenu zaštitnih lozinki i izbjegavanje rizika od računalnih virusa,
- izvješćivanje nadređenog zaposlenika o prekršajima i pokušajima prekršaja sigurnosti,
- izvješćivanje nadređenog zaposlenika o inficiranju ili sumnji o inficiranju računalnim virusom,
- provođenje lokalnih procedura vodeći pritom računa o sigurnosti informacija,
- primjerenu zaštitu informacija uključujući i one koje su u ranom stadiju pripreme ili diskusije i ne mogu još formalno biti zabilježene u informacijski sustav,
- siguran prijenos informacija na način koji minimizira rizik slučajne ili namjerne zlouporabe izvan NCARH.

5.3. Privatnost

Za čuvanje privatnosti osobnih informacija odgovornost je na svim zaposlenicima OA NCARH. Važno je za svakog zaposlenika da poštuje privatnost drugih.

Kada pristupna prava i ovlasti dopuštaju pristup osobnim informacijama koje drži NCARH u računalnom formatu, pristup će bit odobren jedino kada je stvarna potreba za tim radi izvršavanja zaposlenikovih zadaća.

Prilikom revizija bit će potrebno da specijalist sigurnosti pristupi i e-mailovima pohranjenim na NCARH uređajima, iz sigurnosnih razloga.

Pristup će se drugim datotekama korisnika izbjegavati, osim ako to nije direktno vezano uz radne zadaće.

Zaposlenici koji pristupe bilo kojem dijelu mreže bez potrebne ovlasti, mogu biti disciplinski ili sudski gonjeni.

Zaposlenik ne može pristupiti ili otkriti osobne ili tajne informacije, osim u iznimnim okolnostima. Te okolnosti uključuju, ali nisu limitirane na sljedeće:

- pristanak osobe na koju se informacija odnosi,
- na zahtjev nadležnog suda,
- u skladu s nekim drugim zakonskim obavezama.

U svim će ovim slučajevima davanje informacija nadgledat i odobrvat PMA HR PKI.

5.4. Školovanje i obuka

Obuka za područje sigurnosti je bitan element za postizanje znanja i vještina potrebnih za osoblje. Obuku osoblja treba provoditi učestalo da bi osoblje postalo svjesno svojih obaveza i odgovornosti u odnosu na sigurnost.

Na voditelju je OA NCARH da osigura školovanje za područje sigurnosti.

Ova obuka uključuje školovanje svih novih članova osoblja o Općim pravilima sigurnosti te potpuno objašnjenje svih odgovornosti.

Nove sigurnosne procedure ne smiju biti uvedene bez odgovarajućeg programa školovanja koji osigurava upoznavanje osoblja s njihovim novim odgovornostima.

5.5. Računala i SW u privatnom vlasništvu

Opremu u privatnom vlasništvu zabranjeno je priključiti na NCARH računalni sustav. Nema iznimki za ovo pravilo.

Prenosiva računala koje upotrebljavaju osobe pod ugovorom ne smiju se priključiti na produkcijsku mrežu, prije priključka mora se provjeriti je li instalirana ažurna verzija programa za detekciju i zaštitu od virusa.

Korištenje privatnih promjenjivih medija pri priključivanju na NCARH sustav je zabranjena.

NCARH

Opća pravila o sigurnosti

Sva su NCARH računala konfigurirana za standardiziranu operativnu okolinu. Promjenu ove okoline, odnosno dodavanje, brisanje ili promjenu SW mora dopustiti voditelj OA NCARH-a.

5.6. Autorska prava na SW

Autorska prava ograničavaju načine upotrebe SW-a i podataka. Bilo koje narušavanje autorskih prava može izazvati sudski postupak protiv osobe i/ili tvrtke. Cjelokupno osoblje OA NCARH-a mora se pridržavati pravila, da SW zaštićen autorskim pravima i pripadajući materijal, upotrebljavaju u skladu s uvjetima licenci koje se na to odnose. Osoblje smije koristiti samo autorizirani SW. To znači SW koji je legalno nabavljen ili razvijen, i upotrebljava se u skladu s uvjetima nabave.

Sistemske administratore moraju osigurati primjenu i održavanje mehanizama koji provjeravaju je li upotrebljavan samo autorizirani SW. Takve će se provjere i postupci učestalo provoditi. Bilo koji neautorizirani SW otkriven na mreži odmah treba prijaviti voditelju OA NCARH-a.

Voditelj OA NCARH mora osigurati da svi zaposlenici budu obaviješteni o zahtjevima politike autorskih prava te propisanim procedurama koje treba slijediti.

5.7. Elektronička pošta

Elektroničku poštu koriste kao pomoć zaposlenici u svakodnevnom izvršavanju svojih zadataka. Ako se elektronička pošta koristi za slanje osobnih poruka, one će biti tretirane kao i poruke koje se odnose na posao, NCARH pridržava pravo pristupa bilo kojoj osobnoj poruci, njezina kopiranja, brisanja ili otkrivanja takve poruke ako je potrebno i to smatra primjerenim.

Osobna upotreba ne smije:

- preklapati se s normalnim radnim aktivnostima,
- biti povezana s nekom vanjskom poslovnom aktivnošću,
- biti za bilo koju aktivnost koja može ugroziti NCARH.

Ako je primljena bilo kakva poruka koja je uvredljiva, anonimna ili se čini da je primljena od nekoga tko nije pravi pošiljatelj, o tome treba obavijestiti voditelja. Takva se poruka briše nakon odobrenja voditelja.

Svaka je zlouporaba e-mail sustava neprihvatljiva i to povlači sankcije ili druge disciplinske akcije.

5.8. Sankcije

Ako se otkrije da je autorizirani zaposlenik zloupotrijebio resurse na koje mu je bio odobren pristup i/ili je izvršio aktivnosti štetne za sigurnost tih resursa, takva aktivnost mora biti dokumentirana i o tome mora biti obaviješten voditelj OA NCARH-a, koji treba o tome obavijestiti PMA.

Sankcije će protiv zaposlenika pod ugovorom biti u skladu s odredbama ugovora.

Ovisno o prirodi zaposlenikove akcije, sankcije se mogu kretati od savjetovanja ili suspenzije prava pristupa sustavu do otkaza i/ili pravne akcije.

6. UPRAVLJANJE NCARH SUSTAVOM

6.1. Kontrola upravljanja

Kontrola je upravljanja uvedena da bi se osiguralo da promjene konfiguracije ne proizvedu samo željeni učinak nego da, također, osiguravaju i normalan nastavak dnevnih aktivnosti. Jedan je od takvih zahtjeva sigurnost. Stoga kontrola izmjene konfiguracije osigurava da predložene promjene na temeljnoj konfiguraciji ne degradiraju sigurnost sustava na bilo koji način. Sve promjene temeljne konfiguracije zahtijevaju ponovnu procjenu rizika i opasnosti.

Kontrola će se izmjene konfiguracije provoditi da bi se nadgledao sve promjene temeljne konfiguracije na računalima, na svim NCARH mrežama, uključujući:

- HW promjene,
- SW promjene,
- dokumentaciju HW i SW promjena.

Potpuno je dokumentirana temeljna konfiguracija uspostavljena za NCARH. Ova se konfiguracija nadopunjuje na istovjetan način za cijeli sustav.

PMA HR PKI će odobravati sve promjene NCARH konfiguracije.

Sve promjene na temeljnoj konfiguraciji bilo da se radi o HW, SW ili dokumentaciji moraju biti zabilježene **mehanizmom kontrole promjena**.

6.2. Povjerenstvo za kontrolu promjena

Povjerenstvo za kontrolu promjena čine:

- predstavnici PMA HR PKI,
- predstavnici OA NCARH:
 - *osoblje zaduženo za sigurnost,*
 - *sistem administratori,*
 - *osoblje zaduženo za operativni rad.*

Ovo povjerenstvo mora razmotriti svaku promjenu u HW, SW ili procedurama i utjecaj svake promjene na sigurnost i raspoloživost mreže. Jednom kad je dopuštenje za promjenu dano, zahtjev za promjenu se prosljeđuje PMA HR PKI za konačnu autorizaciju.

Promjene se ne smiju provesti prije nego što PMA izvrši njihovu autorizaciju.

6.2.1. Kontrola SW

Kontrola SW uključuje odabir SW, instalaciju, razvoj i dokumentiranje. Povjerenstvo za kontrolu promjena nadzire sav operativni SW NCARH. Jedina iznimka su programi koji se

upotrebljavaju za svrhe razvoja, koji se mogu koristiti samo u razvojnoj okolini, odvojeno od produkcijske mreže.

6.3. Operacije

Transportni mehanizmi za ključeve i certifikate osiguravaju da isključivo pravi vlasnici dobivaju privatne ključeve i njihove certifikate, te da autorizirani korisnici dobivaju javne ključeve.

Uspostavljen je X.500 imenik koji omogućuje pristup statusima certifikata i javnim ključevima.

Pripremljena je dokumentacija za planiranje i održavanje da bi se osigurala pravilna operativnost servisa. Minimalna dokumentacija sadrži:

- koncept operacija,
- procjenu rizika i opasnosti,
- plan sigurnosti informatičkog sustava,
- plan za oporavak u slučaju nezgode,

6.4. Tehnologija

NCARH, CA-i i RA-i čine PKI hijerarhiju.

NCARH će raditi u skladu sa sigurnosnim standardima, što pokriva sljedeća područja:

- pripremu,
- okolinu,
- tehničku sigurnost,
- inspekciju i izvješćivanje o sigurnosti,
- poseban značaj mreže,
- sigurnost malih sustava,
- ostala područja.

Nitko od OA NCARH osoblja ne smije:

- koristiti bilo koji računalni ili mrežni uređaj bez točne autorizacije,
- pomagati, ohrabriti bilo koju neautoriziranu upotrebu ili pokušaj neautorizirane upotrebe računalnog ili mrežnog uređaja,
- svjesno dovesti u opasnost sigurnost bilo kojeg računala ili mrežnog uređaja,

7. SIGURNOST INFRASTRUKTURE

7.1. Sigurnost mreže

Standardi koji se primjenjuju za sigurnost mreže za NCARH računalni sustav su u skladu s međunarodnim standardima. Fizički pristup komunikacijskoj opremi odobrava voditelj OA NCARH.

Da bi se osigurala sigurna mrežna okolina, NCARH produkcijska mreža oblikovana je upotrebom kombinacije vatrozidova, visoko raspoloživog SW za vatrozid i sustava za otkrivanje pokušaja upada. S namjenskim sustavom za upravljanje mrežom, nadziranje u realnom vremenu cijele mrežne infrastrukture, operativnom osoblju osigurano je upozorenje (alert) ako se nešto događa na mreži.

Također postoji sustav bilježenja ako se dogodi bilo koji incident na mreži.

7.2. Konfiguracija vatrozida (FIREWALL)

Konfiguracija vatrozidova na NCARH produkcijskoj mreži smatra se sa stanovišta sigurnosti posebno osjetljivom i zato je klasificirana kao "**visoko zaštićena**". Samo voditelj OA NCARH, glavni korisnik i specijalist sigurnosti imaju pristup tim informacijama.

8. SIGURNOST PODATAKA

Vlasnik je informacije odgovoran da se podaci koji se nalaze pod njegovom kontrolom klasificiraju u skladu s njihovom tajnošću, osjetljivošću i kritičnošću.

8.1. Obilježavanje i pohranjivanje osjetljivih medija

Kada se osjetljive informacije zapisuju na disketu, magnetsku vrpču, Smart karticu, CD rom ili druge medije, medij mora biti označen s najvišom klasifikacijom osjetljivošću. Kada nisu u upotrebi, svi mediji s tom klasifikacijom moraju biti pohranjeni u sigurne kontejnere.

8.2. Sigurnost medija

Izraz IT mediji za pohranjivanje odnosi se na magnetske vrpce, kasete, tvrde diskove, diskete, CD romove, DVD i drugu opremu za pohranjivanje podataka.

Sistemske administratori su odgovorni za osiguranje tada, kada IT medij za pohranjivanje bude ponovno korišten ili stavljen izvan upotrebe, ne postoji mogućnost narušavanja tajnosti zbog neautoriziranog pristupa podacima na mediju.

Mediji koji su bili upotrebljavani za pohranjivanje visoko zaštićenih informacija ne smiju se ponovo koristiti za pohranjivanje informacija niže sigurnosne klasifikacije. Voditelj je OA

NCARH

Opća pravila o sigurnosti

NCARH odgovoran za osiguranje IT medija za pohranjivanje, tj. spremanje u sigurne kontejnere.

8.3. Prijenos i pohranjivanje podataka

Bilo koji IT medij za pohranjivanje koji se upotrebljava za prijenos informacija ne smije sadržavati nikakve ostatke informacija za pristup kojima primatelj nema autorizaciju. Ako se prisutnost ostataka informacija na korištenim medijima ne može odrediti, mora se koristiti novi medij za transfer. Mediji za pohranjivanje koji su ranije sadržavali visoko klasificirane informacije ili podatke ostaju rangirani u sigurnosnoj klasifikaciji tih podataka.

8.4. Prenosiva/Laptop računala

Osoba koja je preuzela opremu odgovara za zaštitu NCARH prenosivih računala i podataka koje se nalaze na njima.

Kada se upotrebljavaju za obradu osjetljivih informacija, prenosiva će računala bit konfigurirana tako da zahtijevaju lozinku prilikom prijave.

Svi osjetljivi podaci koji se čuvaju na tvrdom disku prenosivog/laptop računala, enkriptirani su automatskim procesom enkripcije.

Prenosiva/laptop računala trebaju imati ažurne verzije programa za detekciju i zaštitu od virusa.

Prenosiva/laptop računala, kad nisu pod nadzorom, moraju uvijek biti čuvana na sigurnom .

8.5. Računalni virusi

Voditelj je OA NCARH odgovoran:

- da je instalirana zaštita od virusa na sve servere i računala koja rade na svim NCARH mrežama,
- da su nove verzije antivirus programa instalirane na svim računalima i mrežnim poslužiteljima, i to odmah čim su one raspoložive

Svi vanjski mediji koji ulaze u NCARH prostor moraju prije uporabe biti provjereni na viruse, a provjeru provodi osoba zadužena za sigurnost.

Svi korisnici moraju hitno obavijestiti voditelja OA NCARH sumnjaju li na virus ili program koji uništava sadržaj na mediju. Time će se osigurati pravodobno poduzimanje radnji koje će spriječiti daljnje zaraze.

8.6. Arhiva

8.6.1. Tipovi pohranjenih podataka

NCARH arhivira sljedeće tipove podataka, automatski ili ručno:

- događaje koji su predmet revizije,

- certifikate i CRL,
- ključeve,
- izvještaje o kompromitiranosti, neslaganjima i dopisivanju.

8.6.2. Period arhiviranja

NCARH arhivira revizijske logove za najmanje 6 godina. Certifikati, CRL i ključevi se arhiviraju na najmanje 30 godina. NCARH dopisivanje se arhivira najmanje na 10 godina.

9. FIZIČKA ZAŠTITA

Zgrada u kojoj se nalazi NCARH operativni centar je sigurna zgrada, koja ima višeslojne sigurnosne barijere.

Sigurnosna tehnologija koja se koristi u operativnom centru sastoji se od integriranih rješenja suvremenih tehnologija koje zadovoljavaju zahtjeve potpune sigurnosti.

9.1. Vođenje evidencije pristupa NCARH prostoru

Voditelj je OA NCARH odgovoran za vođenje evidencije te održavanje svih kontrola pristupa u NCARH. Izmjene će se u pristupnoj listi održavat ažurno.

9.2. Evidentiranje imovine

Sva se imovina, uključujući računalnu opremu, namještaj i računalni SW evidentira u "**Registru imovine**". Ovaj registar održava voditelj OA NCARH i dopunjava se u sljedećim situacijama:

- instaliranje/deinstaliranje/promjena uređaja,
- postojeća se imovina ne može servisirati zbog:
 - oštećenja,
 - dotrajalosti,
 - promjene u tehnologiji.
- prijenos uređaja na drugu lokaciju tvrtke,
- dogradnja.

Sva je imovina označena s jedinstvenom identifikacijskom oznakom, čiji se detalji bilježe u registru imovine zajedno s punim opisom pojedinog predmeta (komada/dijela)

10. NARUŠAVANJE SIGURNOSTI

10.1. Unutarnje narušavanje sigurnosti

U slučaju unutarnjeg narušavanja IT sigurnosti, od strane zaposlenika, glavni korisnik obavještava PMA.

U takvim situacijama ima više mogućnosti izbora:

- formalni sastanak sa zaposlenikom i otpuštanje ili službena opomena,
- u slučaju industrijske špijunaže, slučaj se može krivično procesuirati.

Svi će relevantni logovi bit potrebni kao evidencija za dalje sudsko procesiranje. Zato oni moraju biti ispravno označeni i spremljeni na sigurnu lokaciju.

Ako NCARH poduzima mjere protiv zaposlenika, treba tražiti pravno mišljenje.

10.2. Vanjsko narušavanje sigurnosti

Dođe li do vanjskog narušavanja sigurnosti NCARH računalne mreže, prvi prioritet je zaustavljanje same te akcije. Ako je osoba pokušala pristupiti mreži, svi naponi moraju biti učinjeni za zaustavljanje tog pristupa. Ako je pristup bio uspješan, tada se mora primijeniti plan za odgovor na kritični incident. U tom su slučaju backupirani logovi važni, jer će to pomoći pri izoliranju prvog pristupa ili bilo kojeg višestrukog pristupa.

Sve log datoteke poslužitelja trebaju biti održavane i pohranjene na sigurnom mjestu.

10.3. Procedure izvještavanja o unutarnjem ili vanjskom narušavanju sigurnosti

U slučaju bilo kakvog unutarnjeg ili vanjskog narušavanja sigurnosti, treba slijediti sljedeće procedure:

- treba obavijestiti voditelja OA NCARH i glavnog korisnika, da bi se poduzele pravodobno akcije,
- PMA HR PKI treba odmah biti detaljno obaviještena o situaciji,
- voditelj OA NCARH i PMA HR PKI moraju odlučiti o smjeru akcije kao što je gore naznačeno,
- specijalist će sigurnosti pretražiti i zadržati sve relevantne log datoteke poslužitelja. U slučaju da su datoteke bile promijenjene one moraju biti izolirane za analize revizora, a za vrijeme ovog procesa trebaju biti izrađene opsežne bilješke o svim poduzetim koracima,
- sistem treba biti vraćen u njegov "originalni" format.

Ako bilo koje narušavanje sigurnosti ima utjecaj na nekog klijenta o tome treba obavijestiti osoblje koje kontaktira s klijentima, da bi bili informirani dođe li do reakcije klijenta.

11. OSIGURANJE KONTINUITETA POSLOVANJA

11.1. Procjena ranjivosti

PMA HR PKI da bi osigurao najviši stupanj sigurnosti poslovanja formira tim za procjenu ranjivosti i saniranje kriznih situacija. Tim se sastoji od:

- člana PMA HR PKI,
- voditelja OA NCARH i glavnih korisnika,
- specijalista sigurnosti.

Tim će provodi reviziju konfiguracije NCARH aplikacijskog i operativnog SW, kao i periodična testiranja konfiguracije vatrozida (firewalla), usmjerivača (routera), podatkovne osnovice i imenika.

11.2. Plan oporavka u slučaju incidenta (Disaster Recovery Plan)

Voditelj OA NCARH operacija je odgovoran za održavanje ažurnih i važećih planova za oporavak u slučaju incidenta. Takovi će planovi bit testirani i pregledavani redovito po nalogu PMA HR PKI-a.

Specijalist sigurnosti odgovoran je za identificiranje rizika i provedbu ponovne procjene rizika.

Osoblje će se prema svojim odgovornostima redovito uvježbavati za provođenje primjerenih procedura za slučaj nezgode.

Backup procedure trebaju biti odgovarajuće, detaljne i aktualne da bi odgovarale potrebama oporavka sustava.

Potrebno je da postoje procedure za vraćanje u normalan rad nakon nezgode.

PMA HR PKI je odgovorna za uspostavu plana za oporavak u slučaju incidenta, što uključuje sljedeće:

- procedure za Backup i arhiviranje koje su dovoljne za obnovu uređaja i kritičnih aplikacija,
- upute za procjenu hitnih situacija i određivanje zahtjeva za rješavanje,
- određivanje uvjeta za prelazak na drugu lokaciju, prelazak na tu lokaciju i povratak na prijašnju lokaciju,
- procedure za backup i recovery podataka i SW,
- procedure za testiranje.

Cjelokupno osoblje koje bi radilo u ovakvim situacijama mora biti informirano o svojim odgovornostima i mora biti redovito obučavano za svoje zadaće.

Plan za oporavak u slučaju nezgode i plan za nastavak posla su izrađeni tako da bi osigurali pravodoban oporavak za nastavak rada u slučaju velikih nezgoda. Plan osigurava brzi nastavak bitnih operacija.

Plan mora biti redovito testiran da bi se provjerila izvedivost. Scenarij će za provjeru plana biti izrađen, te će se naznačiti kako i kada će se pojedini elementi plana provjeriti.

Plan zbog promjena u poslovanju zastarijeva brzo i zbog toga će biti dopunjavan dva puta godišnje da bi se osigurala njegova stalna učinkovitost.

Primjeri izmjena koje mogu nastati su ovi:

- nova oprema,
- dopuna ili promjena operativnog sustava,
- primjena nove tehnologije za kontrolu i detekciju,
- promjene u osoblju,
- promjene ugovornih odnosa i isporučitelja,
- promjena telefonskih brojeva i adresa,
- prestanak rada, izmjena ili uvođenje novih poslovnih procesa,
- promjena u postupcima rada na sustavu,
- promjene u zakonskoj regulativi.

11.3. Odaziv na kritične incidente

PMA HR PKI formira tim za odaziv na kritične incidente, da bi pravodobno odgovorili na kritične incidente, te da bi se primijenio plan za oporavak u slučaju nezgode. Tim se sastoji od člana PMA HR PKI, voditelja OA NCARH i glavnog korisnika.

Zadatak tima je:

- odrediti pristupne točke resursima,
- minimalizacija učinka bilo kojeg incidenta na NCARH poslovnu praksu,
- primjena strategija za minimiziranje štete,
- hitna reakcija na incident,
- prikupljanje podataka za disciplinske postupke,
- izvještavanje PMA.

Neki incidenti zahtijevaju taktičke odluke, primjerice, prekid aktivnosti koja je izazvala incident, a. koje će donijeti PMA HR PKI, vodeći računa o sljedećem:

- apsolutni prioritet je minimiziranje rizika ili opasnosti za NCARH sustav,
- identificiranje slabosti u sustavu,
- identificiranje osoba koje su sudjelovale,
- važnost prikupljenih informacija.

Voditelj OA NCARH vodi evidenciju za sve kritične incidente. Tu dokumentaciju pregledava PMA HR PKI i ona se čuva za potrebe revizije.