NN 46/2008 (23.4.2008.), Uredba o mjerama informacijske sigurnosti

VLADA REPUBLIKE HRVATSKE

1547

Na temelju članka 7. Zakona o informacijskoj sigurnosti (»Narodne novine«, broj 79/2007), Vlada Republike Hrvatske je na sjednici održanoj 18. travnja 2008. godine, donijela

UREDBU

O MJERAMA INFORMACIJSKE SIGURNOSTI

I. OSNOVNE ODREDBE

Članak 1.

Ovom Uredbom utvrđuju se mjere informacijske sigurnosti za postupanje s klasificiranim i neklasificiranim podacima.
Ova Uredba primjenjuje se na državna tijela, tijela jedinica lokalne i područne (regionalne) samouprave, te na pravne osobe s javnim ovlastima, koje u svom djelokrugu koriste klasificirane i neklasificirane podatke.
Ova Uredba primjenjuje se i na pravne i fizičke osobe, koje ostvaruju pristup ili postupaju s klasificiranim i neklasificiranim podacima.

Članak 2.

Pojedini pojmovi u smislu ove Uredbe imaju sljedeće značenje:
– *Hardver* – sklopovlje odnosno fizička komponenta informacijskog sustava;
– *Klasificirani ugovor* – ugovor kojim se razmjenjuju klasificirani podaci između tijela i pravnih osoba iz članka 1. stavka 2. s pravnim i fizičkim osobama iz članka 1. stavka 3.;
– *Kriptomaterijali* – kriptografski proizvodi i podaci, odnosno programska rješenja ili uređaji za zaštitu podataka, tehnička dokumentacija takvih rješenja i uređaja, kao i odgovarajući kriptografski ključevi;
– *Medij za pohranu podataka* – svaki medij na koji je moguće pohraniti podatke u elektroničkom obliku;
– *Opća razina zaštite* – skup mjera i standarda u područjima informacijske sigurnosti propisan za određene stupnjeve tajnosti;
– *Sigurnosna akreditacija sustava registara* – postupak kojim se utvrđuje da li su primijenjene mjere i standardi informacijske sigurnosti propisane za organizaciju rada, osoblje, prostor, informacijske sustave i klasificirane podatke, u prostorima u kojima se organizira prijem, korištenje, pohrana i daljnja distribucija klasificiranih podataka;
– *Sigurnosni spremnik* – sef, kasa te drugi protuprovalno opremljeni prostor za pohranu klasificiranih podataka;
– *Softver* – svi operativni sustavi, programi, korisničke i servisne aplikacije;
– *Ugroza* – potencijalni uzrok koji može nanijeti štetu klasificiranom podatku ili informacijskom sustavu u kojem se koriste klasificirani podaci;

– *Upravljanje rizikom informacijske sigurnosti* – sustavni pristup koji uključuje planiranje, organiziranje i usmjeravanje aktivnosti, s ciljem osiguravanja da rizici za klasificirane podatke ostanu u zakonom utvrđenim i prihvatljivim okvirima;

Članak 3.

Klasificirani podatak štiti se propisanim mjerama i standardima za zaštitu klasificiranih podataka, koje osiguravaju opću razinu zaštite, sve dok je označen jednim od stupnjeva tajnosti.
Kada je procjenom sigurnosnih rizika utvrđeno da su klasificirani podaci izloženi povećanom riziku, tijela i pravne osobe poduzet će potrebne dodatne mjere i standarde za zaštitu istih, sukladno članku 96. ove Uredbe.

Članak 4.

Pristup klasificiranim podacima stupnja tajnosti »Vrlo tajno«, »Tajno« i »Povjerljivo« može ostvariti osoba, koja ima odgovarajući certifikat, koja je upoznata s načinom postupanja s klasificiranim podacima i kojoj je to nužno za obavljanje poslova iz svog djelokruga, a temeljem popisa dužnosti i poslova iz djelokruga.
Pristup klasificiranom podatku stupnja tajnosti »Ograničeno« može ostvariti osoba, koja je upoznata s načinom postupanja s klasificiranim podacima i kojoj je to nužno za obavljanje poslova iz svog djelokruga, a temeljem ovlasti za pristup klasificiranim podacima čelnika tijela ili pravne osobe.

Članak 5.

Klasificirani podatak može se dostavljati drugim tijelima i pravnim osobama, samo uz prethodnu suglasnost vlasnika podatka, i u skladu s ovom Uredbom i pravilnicima, donesenim na temelju zakona.

Članak 6.

Klasificirani podatak može se razmjenjivati samo s državama i međunarodnim organizacijama, koje su potpisale ugovor o uzajamnoj zaštiti klasificiranih podataka s Republikom Hrvatskom.
Iznimno od stavka 1. ovog članka, klasificirani podatak može se razmjenjivati i s državama i međunarodnim organizacijama unutar međunarodne suradnje, koja uključuje razmjenu klasificiranih podataka.
Evidenciju o ugovorima iz stavka 1. ovog članka vodi Ured Vijeća za nacionalnu sigurnost.

Članak 7.

Podatak bez utvrđenog stupnja tajnosti, kad se koristi u službene svrhe, može biti bez oznake ili označen oznakom »Neklasificirano«.
Podatak koji je bez oznake, nema ograničenja uporabe i pristupa osoba.
Podatak koji je označen oznakom »Neklasificirano« koristi se samo u službene svrhe i može biti dostupan isključivo onim fizičkim osobama, tijelima i pravnim osobama koje imaju potrebu korištenja takvog podatka u službene svrhe i radi obavljanja poslova iz njihova djelokruga.
Svaki podatak koji je Republici Hrvatskoj predala druga država, međunarodna organizacija ili institucija s kojom Republika Hrvatska surađuje, a označen je oznakom »Neklasificirano«, odnosno istovrsnom inozemnom oznakom, u skladu s odgovarajućim međunarodnim ugovorom koji je Republika Hrvatska potpisala, koristi se samo u službene svrhe i može biti dostupan isključivo onim fizičkim osobama, tijelima i pravnim osobama koje imaju potrebu korištenja takvog podatka u službene svrhe i radi obavljanja poslova iz njihovog djelokruga.

Članak 8.

Za zaštitu neklasificiranih podataka, tijela i pravne osobe iz članka 1. stavka 2. ove Uredbe utvrđuju i primjenjuju odgovarajući skup mjera informacijske sigurnosti, sukladno normama za upravljanje informacijskom sigurnošću, HRN ISO/IEC 27001 i HRN ISO/IEC 17799.
Za zaštitu klasificiranih podataka stupnja tajnosti »Ograničeno«, uz norme iz stavka 1. ovog članka, primjenjuju se dodatno i druge mjere propisane ovom Uredbom, drugim propisima ili međunarodnim ugovorima.
Savjetnik za informacijsku sigurnost u tijelima i pravnim osobama iz članka 1. stavka 2. ove Uredbe, uz nadzor primjene normi i mjera iz stavaka 1. i 2. ovog članka, redovito provjerava i usklađenost informacijskog sustava u kojem se koriste neklasificirani podaci i klasificirani podaci stupnja tajnosti »Ograničeno« s propisanim normama, mjerama i standardima informacijske sigurnosti.

Članak 9.

Tijela i pravne osobe, koje postupaju s klasificiranim i neklasificiranim podacima, primjenjuju propisane mjere informacijske sigurnosti radi osiguravanja ujednačene razine zaštite svakog klasificiranog ili neklasificiranog podataka u Republici Hrvatskoj.

Članak 10.

Područja informacijske sigurnosti za koja se propisuju mjere i standardi informacijske sigurnosti su:
– sigurnosna provjera,
– fizička sigurnost,
– sigurnost podatka,
– sigurnost informacijskog sustava,
– sigurnost poslovne suradnje.

II. MJERE INFORMACIJSKE SIGURNOSTI ZA PODRUČJE SIGURNOSNE PROVJERE

Članak 11.

Mjere informacijske sigurnosti za područje sigurnosne provjere su:
– popis dužnosti i poslova za koje je potrebno uvjerenje o sigurnosnoj provjeri (u daljnjem tekstu: certifikat);
– postupak za izdavanje certifikata;
– upitnik za sigurnosnu provjeru;
– pisana suglasnost osobe za koju se provodi sigurnosna provjera;
– izdavanje certifikata;
– sigurnosno informiranje;
– nacionalni registar izdanih certifikata, rješenja o odbijanju izdavanja certifikata i potpisanih izjava o postupanju s klasificiranim podacima;
– registar zaprimljenih certifikata i potpisanih izjava o postupanju s klasificiranim podacima.

Članak 12.

Sve osobe, koje imaju pristup klasificiranim podacima, dužne su najmanje jednom godišnje, pristupati sigurnosnom informiranju o propisanim mjerama i standardima informacijske sigurnosti, te potpisati Izjavu o postupanju s klasificiranim podacima.

Članak 13.

Sigurnosno informiranje osoba za pristup stupnjevima tajnosti »Vrlo tajno«, »Tajno« i »Povjerljivo« provode ovlaštene osobe Ureda Vijeća za nacionalnu sigurnost.
Ured Vijeća za nacionalnu sigurnost može, za poslove iz stavka 1. ovog članka, osposobiti osoblje zaposleno u sustavu registara, savjetnike za informacijsku sigurnost u tijelima i pravnim osobama ili druge sigurnosne koordinatore koje tijela i pravne osobe odrede.
Sigurnosno informiranje osoba za pristup stupnju tajnosti »Ograničeno« provode savjetnici za informacijsku sigurnost u tijelima i pravnim osobama ili drugi sigurnosni koordinatori koje tijela i pravne osobe odrede.

Članak 14.

Tijela i pravne osobe iz članka 1. stavka 2. ove Uredbe, koja postupaju s klasificiranim podacima »Vrlo tajno«, »Tajno« i »Povjerljivo«, dužna su voditi registar zaprimljenih certifikata i potpisanih izjava o postupanju s klasificiranim podacima.
Tijela i pravne osobe iz članka 1. stavka 2. ove Uredbe, koja postupaju s klasificiranim podacima stupnja tajnosti »Ograničeno«, dužna su voditi registar potpisanih izjava o postupanju s klasificiranim podacima.

III. MJERE INFORMACIJSKE SIGURNOSTI ZA PODRUČJE FIZIČKE SIGURNOSTI

Članak 15.

Mjere informacijske sigurnosti za područje fizičke sigurnosti su:
– višestruka zaštita;
– sigurnosne zone;
– administrativne zone;
– plan fizičke sigurnosti;
– procjena učinkovitosti mjera fizičke sigurnosti;
– kontrola osoba;
– pohrana klasificiranih i neklasificiranih podataka;
– tehnički sigurni prostori;
– fizička sigurnost informacijskih sustava;
– oprema za fizičku zaštitu klasificiranih podataka.

Članak 16.

Lokacije, zgrade, uredi, prostorije i druga područja, u kojima se čuvaju ili se postupa s klasificiranim podacima, štite se odgovarajućim mjerama fizičke sigurnosti.

Članak 17.

Mjere fizičke sigurnosti provode se radi:
– sprečavanja neovlaštenog ili nasilnog ulaska osoba,
– odvraćanja, sprečavanja i otkrivanja zlouporaba zaposlenika,
– razdvajanja zaposlenika prema ovlastima za pristup klasificiranim podacima
– otkrivanja i reagiranja na sve sigurnosne ugroze.

Članak 18.

Mjere fizičke sigurnosti određuju se, s obzirom na stupanj tajnosti, broj, oblik i način pohrane klasificiranih podataka, ovlaštenja za pristup klasificiranim podacima, te sigurnosnu prosudbu o mogućim ugrozama.

Članak 19.

Mjere fizičke sigurnosti primjenjuju se koordinirano s mjerama sigurnosti podataka, mjerama sigurnosti informacijskih sustava i mjerama sigurnosne provjere.

Višestruka zaštita

Članak 20.

Mjere fizičke sigurnosti primjenjuju se višestrukom zaštitom kroz:
– određivanje lokacije koju treba zaštititi;
– uspostavljanje sigurnosnih mjera radi zaštite i usporavanja neovlaštenog ulaza;
– određivanje vanjskih mjera fizičke sigurnosti;
– uspostavljanje mjera za utvrđivanje pokušaja neovlaštenog pristupa;
– određivanje mjera fizičke sigurnosti radi usporavanja neovlaštenog pristupa;
– usklađivanje brzine dolaska djelatnika osiguranja s vremenom usporavanja neovlaštenog pristupa.

Sigurnosne zone

Članak 21.

Prostori u kojima se pohranjuju ili se postupa s klasificiranim podacima stupnjeva tajnosti »Vrlo tajno«, »Tajno« i »Povjerljivo«, ustrojavaju se kao Sigurnosna zona I ili Sigurnosna zona II.
Sigurnosna zona I je jasno označen i zaštićen prostor s kontrolom pristupa i s utvrđenim stupnjevima tajnosti klasificiranih podataka i vrstama podataka koji se nalaze u tom prostoru.
Pristup Sigurnosnoj zoni I dozvoljen je osobama koje imaju certifikat i koje imaju ovlaštenje za pristup tom prostoru.
Sigurnosna zona II utvrđuje se na način propisan za Sigurnosnu zonu I.
Pristup Sigurnosnoj zoni II dozvoljen je, pored osoba koje imaju certifikat i ovlaštenje za pristup tako ustrojenom prostoru i drugim osobama, ali samo uz pratnju ili primjereni nadzor i uz opravdan razlog ulaska.

Članak 22.

Kontrola pristupa u sigurnosne zone ostvaruje se provjerom identiteta za posjetitelje, a za zaposlenike uvidom u odgovarajuću službenu iskaznicu ili propusnicu, odnosno odgovarajućim automatskim sustavom kontrole pristupa.

Članak 23.

Odgovorne osobe tijela i pravnih osoba iz članka 1. stavka 2. ove Uredbe, radi zaštite klasificiranih podataka, organiziraju kontrolu sigurnosnih zona na kraju radnog dana.

Administrativne zone

Članak 24.

Administrativna zona se uspostavlja za korištenje neklasificiranih podataka i klasificiranih podataka stupnja tajnosti »Ograničeno«u kontroliranom, vidljivo označenom prostoru unutar kojeg je moguće kontrolirati pristup osoba i vozila.
Administrativna zona uspostavlja se u prilazu sigurnosnoj zoni radi kontrole pristupa.

Plan fizičke sigurnosti

Članak 25.

Tijela i pravne osobe iz članka 1. stavka 2. ove Uredbe, za objekte ili prostore u kojima koriste klasificirane i neklasificirane podatke, izrađuju plan potreba, provedbe i organizacije za primjenu mjera fizičke sigurnosti.

Procjena učinkovitosti mjera fizičke sigurnosti

Članak 26.

Tijela i pravne osobe iz članka 1. stavka 2. ove Uredbe, najmanje jednom godišnje, procjenjuju učinkovitost mjera fizičke sigurnosti i sigurnosnog sustava u cjelini, a obvezno kada dolazi do promjene namjene zaštićene lokacije ili elemenata u sigurnosnom sustavu.

Kontrola osoba

Članak 27.

Tijela i pravne osobe iz članka 1. stavka 2. ove Uredbe, dužne su provoditi povremene kontrole osoba na ulazima i izlazima iz objekata ili prostora, radi sprječavanja neovlaštenog iznošenja klasificiranih podataka ili sprječavanja unošenja nedozvoljenih predmeta.

Pohrana klasificiranih podataka

Članak 28.

Podatak stupnja tajnosti, »Vrlo tajno«, pohranjuje se unutar sigurnosnih zona:
– u odgovarajućem sigurnosnom spremniku, opremljenom sustavom detekcije neovlaštenog pristupa, uz stalnu zaštitu i periodični nadzor, ili
– u prostoru za otvorenu pohranu, koji je opremljenom sustavom detekcije neovlaštenog pristupa.
Podatak stupnja tajnosti, »Tajno«, pohranjuje se unutar sigurnosnih zona:
– u odgovarajućem sigurnosnom spremniku, ili
– u prostoru za otvorenu pohranu, opremljenom sustavom detekcije neovlaštenog pristupa ili stalnom zaštitom i periodičnim nadzorom.
Podatak stupnja tajnosti, »Povjerljivo«, pohranjuje se unutar sigurnosnih zona, u odgovarajućem sigurnosnom spremniku.
Podatak stupnja tajnosti, »Ograničeno« i podatak označen oznakom »Neklasificirano«, pohranjuje se u uredski namještaj koji se zaključava.

Tehnički sigurni prostori

Članak 29.

Tehnički sigurni prostori su objekti ili prostorije unutar sigurnosnih zona u kojima se postupa s podacima stupnja tajnosti »Vrlo tajno«i »Tajno«, čiji ulaz se posebno kontrolira i koji su protuprislušno zaštićeni.
Tehnički sigurni prostori, kada nisu u uporabi, moraju biti zaključani i čuvani, u skladu sa standardima fizičke sigurnosti.

Fizička sigurnost informacijskih sustava

Članak 30.

Informacijski sustavi u kojima se obrađuju, pohranjuju ili prenose klasificirani podaci stupnjeva tajnosti »Vrlo tajno«, »Tajno« i »Povjerljivo« instaliraju se unutar sigurnosnih zona.
Prostori u kojima se nalaze poslužitelji, komunikacijska ili upravljačka oprema informacijskih sustava u kojima se koriste podaci stupnja tajnosti »Ograničeno«, organiziraju se kao sigurnosne zone.
Prostori u kojima se putem informacijskih ili komunikacijskih sustava koriste neklasificirani podaci ili klasificirani podaci stupnja tajnosti »Ograničeno«, organiziraju se kao administrativne zone.

Oprema za fizičku zaštitu klasificiranih podataka

Članak 31.

Oprema za fizičku zaštitu klasificiranih podataka treba biti u skladu sa standardima informacijske sigurnosti za područje fizičke sigurnosti, odnosno s odgovarajućim nacionalnim ili međunarodnim normama.

IV. MJERE INFORMACIJSKE SIGURNOSTI ZA PODRUČJE SIGURNOSTI PODATAKA

Članak 32.

Mjere informacijske sigurnosti za područje sigurnosti podataka su:
– klasificiranje i deklasificiranje podataka;
– označavanje podataka;
– pristup podacima;
– zaštita podataka;
– sustav registara;
– evidencija korištenja klasificiranih podataka;
– postupanje u izvanrednim situacijama;
– ustupanje klasificiranih podataka drugoj državi ili međunarodnoj organizaciji.

Članak 33.

Vlasnik klasificiranog podatka može donijeti internu uputu o načinu obrazloženja dodijeljenog stupnja tajnosti pojedinom klasificiranom podatku ili grupi podataka, a u svrhu provođenja naknadne periodične procjene.
Prilikom nastanka klasificiranog podatka, vlasnik klasificiranog podatka može, kada je to moguće, odrediti rok u kojem se stupanj tajnosti klasificiranog podatka može promijeniti ili u kojem će se klasificirani podatak moći deklasificirati.

Članak 34.

Kada vlasnik podatka za izradu novog klasificiranog podatka koristi klasificirane podatke iz različitih izvora, procijenit će stupanj tajnosti istih, u svrhu određivanja stupnja tajnosti novog klasificiranog podatka.
Dijelovi klasificiranog podatka, stranice, paragrafi, odlomci, prilozi i dodaci, kada se koriste ili distribuiraju, označavaju se izvornim stupnjem tajnosti.
Ukoliko se popratni dopisi kojima se klasificirani podaci dostavljaju, razdvajaju od klasificiranog dokumenta, a ne sadrže klasificirane podatke, označavaju se oznakom »Neklasificirano – razdvojeno od priloga«.

Sustav registara

Članak 35.

Sustav registara za razmjenu klasificiranih podataka s drugim državama i međunarodnim organizacijama, čine:
– Središnji registar u Uredu Vijeća za nacionalnu sigurnost,
– podregistri Središnjeg registra,
– registri, u drugim tijelima i pravnim osobama iz članka 1. stavka 2. ove Uredbe.

Članak 36.

Registri iz članka 35. alineje 3. ustrojavaju se u tijelima i pravnim osobama, za internu distribuciju klasificiranih podataka, u koordinaciji s Uredom Vijeća za nacionalnu sigurnost.
Povremeni pristup klasificiranim podacima ne zahtijeva ustrojavanje registra, ukoliko se provode propisane mjere i standardi zaštite klasificiranih podataka, te ukoliko se vodi evidencija krajnjih korisnika podataka.

Članak 37.

Ured Vijeća za nacionalnu sigurnost provodi sigurnosnu akreditaciju sustava registara, te izdaje certifikat kojim odobrava rad i određuje najviši stupanj tajnosti klasificiranih podataka s kojima se može postupati.
Ured Vijeća za nacionalnu sigurnost utvrđuje valjanost akreditacije iz stavka 1. ovog članka, najmanje jednom u dvije godine.

Članak 38.

Središnji registar, podregistri Središnjeg registra i registri, kada postupaju s klasificiranim podacima stupnja tajnosti »Vrlo tajno« dužna su odrediti nadzornog službenika.

Članak 39.

Registar za evidenciju, nadzor i distribuciju kriptografskog materijala sastavni je dio Zavoda za sigurnost informacijskih sustava, a podaci koji se prenose ovim putem ne zahtijevaju evidentiranje kroz sustav registara.

Evidencija korištenja klasificiranih podataka

Članak 40.

Tijela i pravne osobe iz članka 1. stavka 2. ove Uredbe, kada koriste klasificirane podatke stupnjeva tajnosti »Vrlo tajno«, »Tajno« i »Povjerljivo«, dužne su voditi evidenciju korištenja propisanu u članku 96. ove Uredbe.

Postupanje u izvanrednim situacijama

Članak 41.

Tijela i pravne osobe koje postupaju s klasificiranim podacima, izrađuju Plan postupanja s klasificiranim podacima u izvanrednim situacijama.

Članak 42.

Kad je klasificirani podatak izgubljen ili zagubljen unutar sigurnosnih ili administrativnih zona, provode se odredbe zakona za slučaj uništenja, otuđenja ili dostupnosti klasificiranog podatka neovlaštenoj osobi.
Ured Vijeća za nacionalnu sigurnost, na temelju saznanja o uništenju, otuđenju ili dostupnosti klasificiranog podatka neovlaštenoj osobi, izvijestit će nadležnu sigurnosno-obavještajnu agenciju i druga nadležna tijela.

Članak 43.

U slučaju uništenja, otuđenja ili dostupnosti klasificiranog podatka druge države ili međunarodne organizacije neovlaštenoj osobi, Ured Vijeća za nacionalnu sigurnost izvijestit će nadležno tijelo druge države ili međunarodne organizacije.

Ustupanje klasificiranih podataka drugoj državi ili međunarodnoj organizaciji

Članak 44.

U slučaju kada je potpisan međunarodni ugovor o uzajamnoj zaštiti klasificiranih podataka, tijela i pravne osobe iz članka 1. stavka 2. ove Uredbe, uspostavljaju suradnju u određenom području, koji uključuje razmjenu klasificiranih podataka, te o razmijenjenim klasificiranim podacima vode posebnu evidenciju.
Tijela i pravne osobe, o uspostavi suradnje i provedbi odredbi međunarodnog ugovora iz stavka 1. ovog članka, izvješćuju Ured Vijeća za nacionalnu sigurnost, najmanje jednom godišnje.

V. MJERE INFORMACIJSKE SIGURNOSTI ZA PODRUČJE SIGURNOSTI INFORMACIJSKOG SUSTAVA

Članak 45.

Mjere informacijske sigurnosti za područje sigurnosti informacijskog sustava su:
– mjere zaštite informacijskog sustava,
– upravljanje sviješću o sigurnosti i
– planiranje djelovanja u izvanrednim okolnostima.

Mjere zaštite informacijskog sustava

Članak 46.

Mjere zaštite informacijskog sustava su:
– zaštita hardvera, softvera i medija za pohranu podataka,
– upravljanje konfiguracijom i sustavom korisničkog pristupa,

– kontrola povezivanja i uporabe informacijskih sustava,
– zaštita od rizika elektromagnetskog zračenja,
– primjena kriptografske zaštite.

Zaštita hardvera, softvera i medija za pohranu podataka

Članak 47.

Hardver i mediji za pohranu podataka štite se i pohranjuju, u skladu s procedurama definiranim za zaštitu podataka najvišeg stupnja tajnosti, koji se na predmetnom hardveru i mediju obrađuju ili pohranjuju.

Članak 48.

Popravak, otpis dotrajalog ili neispravnog hardvera, održavanje, te postupci vezani uz brisanje, popravak i uništenje medija za pohranu podataka, provode se u skladu s propisanim procedurama.

Članak 49.

Obavezna je uporaba softvera u svrhu održavanja cjelovitosti, raspoloživosti i dostupnosti klasificiranih podataka i softvera iz članka 2. alineja 7. ove Uredbe.

Članak 50.

Sustavi za obradu klasificiranih podataka postavljeni su na način koji podrazumijeva isključivanje svih nepotrebnih servisa, uklanjanje svih programa koji nisu potrebni za obavljanje poslovnog procesa korisnika, te instaliranje tekućih sigurnosnih programskih zakrpa.
Upravljanje konfiguracijom i sustavom korisničkog pristupa

Članak 51.

Upravljanje konfiguracijom tijekom planiranja, projektiranja, izgradnje, uporabe, održavanja i prestanka rada informacijskog sustava, mora osiguravati ispunjavanje operativnih i sigurnosnih zahtjeva.

Članak 52.

Upravljanje sustavom korisničkog pristupa podrazumijeva razvijanje, primjenu i održavanje sustava, na način koji omogućuje jednoznačno identificiranje, autentificiranje i autoriziranje korisnika.
Kontrola povezivanja i uporabe informacijskih sustava

Članak 53.

Kontrola povezivanja informacijskih sustava obuhvaća definiranje uvjeta povezivanja informacijskih sustava, te evidentiranje i nadzor istog.

Članak 54.

Kontrola uporabe informacijskih sustava podrazumijeva evidentiranje aktivnosti korisnika informacijskog sustava.
Pored aktivnosti iz stavka 1. ovog članka, primjenjuju se mjere za spriječavanje zlouporabe informacijskih

sustava kroz instaliranje sustava za otkrivanje neovlaštenog upada u mrežu, definiranje, pregledavanje i analiziranje zapisnika rada sustava i provođenje analiza ranjivosti informacijskog sustava.

Zaštita od rizika elektromagnetskog zračenja

Članak 55.

Sva oprema pomoću koje se obrađuju klasificirani podaci stupnja tajnosti »Vrlo tajno«, »Tajno« i »Povjerljivo«, osigurava se TEMPEST protumjerama, u skladu s procjenom rizika od neželjenog elektromagnetskog zračenja.

Primjena kriptografske zaštite

Članak 56.

Povjerljivost, cjelovitost, izvornost i neporecivost klasificiranih podataka, osigurava se korištenjem odobrenih kriptografskih metoda, od strane nadležnog tijela.
Klasificirani podaci tijekom prijenosa štite se metodama iz stavka 1. ovog članka, osim kada je međunarodnim ugovorom o uzajamnoj zaštiti klasificiranih podataka, koji je Republika Hrvatska potpisala s nekom državom ili međunarodnom organizacijom, uređeno drugačije.

Članak 57.

Kad nastupe izvanredne okolnosti koje mogu dovesti u pitanje prijenos klasificiranih podataka propisanim metodama, klasificirani podaci stupnja tajnosti »Tajno«, »Povjerljivo« i »Ograničeno« mogu se prenositi i nekriptirani, uz pisano odobrenje.
Odobrenje iz stavka 1. ovog članka daje čelnik tijela ili pravne osobe ili osoba koju on za to ovlasti, na temelju procjene da će moguće štetne posljedice proizašle iz prijenosa klasificiranih podataka, koji nije u skladu s propisanim metodama, biti manje od onih koje bi proizašle ukoliko do takvog prijenosa ne dođe.

Članak 58.

Tijela i pravne osobe iz članka 1. stavka 2. ove Uredbe, koje koriste kriptografsku opremu i dokumente za zaštitu klasificiranih podataka, primjenjuju sigurnosne mjere, u skladu s propisanim procedurama.

Upravljanje sviješću o sigurnosti

Članak 59.

Upravljanje sviješću o sigurnosti podrazumijeva:
– uspostavljanje sigurnosnih pravila za djelatnike,
– sigurnosno educiranje i stručno usavršavanje.

Uspostavljanje sigurnosnih pravila za djelatnike

Članak 60.

Svi korisnici informacijskog sustava upoznat će se sa sigurnosnim pravilima i posljedicama nepridržavanja istih.

Sigurnosno educiranje i stručno usavršavanje

Članak 61.

Sa svim korisnicima informacijskog sustava, ovisno o vlastitim zaduženjima i odgovornostima, provodi se redovito i pravovremeno educiranje o sigurnosnim aspektima uporabe informacijskog sustava.

Planiranje djelovanja u izvanrednim okolnostima

Članak 62.

Planiranje djelovanja u izvanrednim okolnostima podrazumijeva:
– izradu procedura za postupanje u slučaju incidenata,
– izradu plana neprekidnosti poslovanja.

Izrada plana neprekidnosti poslovanja

Članak 63.

Planiranjem djelovanja u izvanrednim okolnostima utvrđuju se i analiziraju potencijalni problemi pri radu sustava i definiraju se postupci za rješavanje tih problema, te definiraju druge metode korištenja, u slučaju nedostupnosti resursa informacijskog sustava, u cilju održavanja kontinuiteta poslovanja.

Članak 64.

Kontinuitet poslovanja obuhvaća i uspostavljanje i testiranje adekvatne procedure sigurnosne pohrane podataka, radi vraćanja sustava i podataka u prvobitno stanje nakon incidenta (ispad sustava, prirodne nepogode i djelovanje računalnih virusa).

Izrada procedura za postupanje u slučaju incidenata

Članak 65.

Izrada procedura za postupanje u slučaju incidenta podrazumijeva planiranje i definiranje aktivnosti odvraćanja, sprečavanja, detekcije i oporavka od učinaka incidenta, koji utječu na povjerljivost, cjelovitost i dostupnost podatka ili informacijskog sustava, uključujući i izvještavanje o sigurnosnim incidentima.

Članak 66.

Učinkovitost mjera iz članka 45. ove Uredbe, osigurava se sustavnim pristupom koji uključuje:
– razmatranje sigurnosnih aspekata u svim fazama životnog ciklusa informacijskog sustava;
– definiranje odgovornosti za provedbu svake od mjera;
– redovnu kontrolu uspostavljenih sigurnosnih pravila i provedbe istih, u cilju provjere efikasnosti i svrsishodnosti.

VI. MJERE INFORMACIJSKE SIGURNOSTI ZA PODRUČJE SIGURNOSTI POSLOVNE SURADNJE

Članak 67.

Mjere informacijske sigurnosti za područje sigurnosti poslovne suradnje su:
– sklapanje klasificiranih ugovora;
– certifikat poslovne sigurnosti;
– sigurnosni uvjeti za sklapanje klasificiranih ugovora;
– prijevoz klasificiranog materijala;
– pristup klasificiranim podacima prilikom međunarodnih posjeta;
– razmjena osoba u sklopu projekata ili programa.

Sklapanje klasificiranih ugovora

Članak 68.

Tijela i pravne osobe iz članka 1. stavka 2. ove Uredbe, prilikom sklapanja klasificiranih ugovora, u okviru kojih se razmjenjuju klasificirani podaci, sastavljaju dokumentaciju za nadmetanje, na način da sadrži neklasificirane podatke ili podatke stupnja tajnosti »Ograničeno«.
Tijela i pravne osobe iz članka 1. stavka 2. ove Uredbe, dužne su, s pravnim osobama koje su se javile na nadmetanje za klasificirani ugovor, potpisati Izjavu o zaštiti klasificiranih podataka iz natječajne dokumentacije.

Članak 69.

Pravna osoba, kao stranka u klasificiranom ugovoru stupnja tajnosti »Vrlo tajno«, »Tajno« i »Povjerljivo«, dužna je posjedovati certifikat poslovne sigurnosti, a zaposlenici pravne osobe, koji će imati pristup klasificiranim podacima, moraju posjedovati odgovarajući certifikat, te mogu ostvariti pristup samo onim klasificiranim podacima koji su predmet ugovora i koji su im nužni u okviru njihovog djelokruga.
Klasificirani ugovor stupnja tajnosti »Ograničeno«, umjesto certifikata poslovne sigurnosti, mora sadržavati klauzulu o uzajamnoj zaštiti klasificiranih podataka, a zaposlenici pravne osobe, koji će imati pristup klasificiranim podacima, moraju biti sigurnosno informirani i potpisati Izjavu o postupanju s klasificiranim podacima.

Certifikat poslovne sigurnosti

Članak 70.

Zahtjev za izdavanje certifikata poslovne sigurnosti za pravne osobe, radi sklapanja klasificiranih ugovora stupnjeva tajnosti »Vrlo tajno«, »Tajno« i »Povjerljivo«, tijela i pravne osobe iz članka 1. stavka 2. ove Uredbe, dostavljaju Uredu Vijeća za nacionalnu sigurnost.

Članak 71.

Pravne osobe, kad sudjeluju u međunarodnim klasificiranim ugovorima, podnose Uredu Vijeća za nacionalnu sigurnost zahtjev za izdavanje certifikata poslovne sigurnosti, nakon što je certifikat zatražilo nadležno sigurnosno tijelo druge države ili međunarodne organizacije.

Članak 72.

Zahtjev za izdavanje certifikata poslovne sigurnosti sadrži:
– naziv, adresu i matični broj pravne osobe za koju se traži certifikat;
– razlog zbog kojeg se traži certifikat;

– stupanj tajnosti klasificiranih podataka za koje se traži certifikat;
– u cijelosti popunjen i ovjeren Upitnik za sigurnosnu provjeru pravne osobe.

Članak 73.

Postupak izdavanja certifikata poslovne sigurnosti započinje potpisivanjem ugovora između Ureda Vijeća za nacionalnu sigurnost i pravne osobe.
Ugovorom iz stavka 1. ovog članka uredit će se, između ostalog, davanje suglasnosti za provođenje sigurnosne provjere za pravnu osobu, dostavljanje upitnika za sigurnosnu provjeru osoba u pravnoj osobi, koje će imati pristup klasificiranim podacima, te dostava ostale potrebne dokumentacije ili provođenje drugih radnji iz ugovora.
Uputa za provedbu mjera i standarda informacijske sigurnosti za zaštitu klasificiranih podataka u pravnoj osobi sastavni je dio ugovora iz stavka 1. ovog članka.

Članak 74.

Sigurnosna provjera pravne osobe obuhvaća:
– provjeru vlasništva, provjeru strukture vlasništva, podatke o tvrtkama u vlasništvu, provjeru ukupnog poslovanja, te financijskih obveza, s obzirom na moguće sigurnosne rizike;
– sigurnosnu provjeru vlasnika, direktora, članova uprave i nadzornog odbora, udjeličara i dioničara, koji, s obzirom na svoju funkciju, mogu ostvariti pristup klasificiranim podacima;
– sigurnosnu provjeru osobe, predložene za savjetnika za informacijsku sigurnost u pravnoj osobi, za njegova zamjenika, te zaposlenike koji ostvaruju pristup klasificiranim podacima.

Članak 75.

Ured Vijeća za nacionalnu sigurnost izdaje certifikat poslovne sigurnosti pravnoj osobi kada, na temelju izvješća nadležne sigurnosno-obavještajne agencije, utvrdi da ne postoje sigurnosne zapreke i ukoliko su primijenjene mjere i standardi informacijske sigurnosti iz članka 73. stavka 3. ove Uredbe.

Članak 76.

Ured Vijeća za nacionalnu sigurnost izdaje certifikat poslovne sigurnosti u roku, ne dužem od šest mjeseci, od zaključivanja ugovora iz članka 73. ove Uredbe.

Članak 77.

Certifikat poslovne sigurnosti izdaje se na razdoblje od 5 godina.
Za vrijeme važenja certifikata iz stavka 1. ovog članka, Ured Vijeća za nacionalnu sigurnost provodi postupak suspenzije ili ukidanja certifikata, kada se promijene uvjeti utvrđeni ugovorom iz članka 73. ove Uredbe.

Članak 78.

Pravna osoba koja zapošljava stranog državljana na radnom mjestu koje zahtijeva pristup klasificiranim podacima dužna je, posredstvom Ureda Vijeća za nacionalnu sigurnost, zatražiti dostavu certifikata od nadležnog tijela države čija je osoba državljanin.

Članak 79.

Obrazac certifikata iz članka 77. stavka 1. ove Uredbe donosi Ured Vijeća za nacionalnu sigurnost, nalazi se u prilogu ove Uredbe i čini njen sastavni dio.
Obrazac odgovarajućeg međunarodnog certifikata poslovne sigurnosti donosi, za svaki pojedinačni slučaj, Ured Vijeća za nacionalnu sigurnost, sukladno standardima, utvrđenim u okviru međunarodnih ugovora, koje Republika Hrvatska potpisuje s drugim državama i međunarodnim organizacijama.

Sigurnosni uvjeti za sklapanje klasificiranih ugovora

Članak 80.

Prilikom sklapanja klasificiranog ugovora državna tijela i pravne osobe iz članka 1. stavka 2. ove Uredbe, dužni su izraditi, kao prilog ugovoru, naputke o sigurnosnim mjerama u projektu i klasificiranju podataka u projektu.
Međunarodni klasificirani ugovori moraju sadržavati Projektno-sigurnosnu uputu, čiji je sastavni dio Uputa o klasificiranju podataka u projektu.

Prijevoz klasificiranog materijala

Članak 81.

Sigurnosne mjere iz članka 80. provode se kontinuirano za vrijeme prijevoza klasificiranog materijala, pri čemu zaštita klasificirane pošiljke treba biti usklađena s najvišim stupnjem tajnosti pojedinog klasificiranog podatka u pošiljci.
Pravna osoba, kad obavlja prijevoz klasificiranog materijala stupnjeva tajnosti »Vrlo tajno«, »Tajno« i »Povjerljivo«, dužna je posjedovati certifikat poslovne sigurnosti, a osoblje koje postupa s pošiljkom, odgovarajući certifikat o sigurnosnoj provjeri.
Prijevoz se mora odvijati točno utvrđenom rutom, od polazišta do odredišta, mora biti obavljen u najkraćem mogućem roku, te mora sadržavati mjere za sprječavanje neovlaštenog pristupa klasificiranim podacima.

Članak 82.

Plan prijevoza klasificiranog materijala unutar Republike Hrvatske dogovaraju ugovorne stranke, sukladno članku 81. ove Uredbe.

Članak 83.

Plan prijevoza klasificiranog materijala kod međunarodnih klasificiranih ugovora predlaže ugovorna stranka koja je naručitelj prijevoza.
Iznimno od stavka 1. ovog članka, ukoliko je više istovrsnih prijevoza organizirano u kraćem vremenskom razdoblju, moguće je izraditi jedinstveni plan prijevoza.
Ured Vijeća za nacionalnu sigurnost odobrava plan prijevoza i daje suglasnost za međunarodni prijevoz klasificiranog materijala, kada je to propisano međunarodnim ugovorom.

Pristup klasificiranim podacima prilikom međunarodnih posjeta

Članak 84.

Tijela i pravne osobe, kad upućuju zaposlenike u međunarodne posjete, u okviru kojih će imati pristup klasificiranim podacima stupnjeva tajnosti »Vrlo tajno«, »Tajno« i »Povjerljivo«, prijavljuju iste nadležnom tijelu te države ili međunarodne organizacije, posredstvom Ureda Vijeća za nacionalnu sigurnost, ukoliko je potpisan međunarodni ugovor o uzajamnoj zaštiti klasificiranih podataka.
Ured Vijeća za nacionalnu sigurnost izdaje tijelima i pravnim osobama sigurnosna odobrenja, za posjete predstavnika drugih država, međunarodnih organizacija i pravnih osoba, prilikom kojih će imati pristup klasificiranim ugovorima, programima i projektima, na temelju posjedovanja odgovarajućih certifikata, ukoliko je potpisan međunarodni ugovor o uzajamnoj zaštiti klasificiranih podataka.
Ugovorne stranke iz pojedinih programa ili projekata iz klasificiranih ugovora, u okviru kojih se provodi međunarodni posjet, odgovorne su za pokretanje procedure u Uredu Vijeća za nacionalnu sigurnost, koja uključuje obavještavanje o posjeti, te razmjenu odgovarajućih certifikata s nadležnim tijelom u drugoj državi ili međunarodnoj organizaciji.
Tijela i pravne osobe, kad primaju posjete iz stavka 2. ovog članka, vode evidencije posjeta i pristupa osoba klasificiranim podacima.

Članak 85.

Iznimno od članka 83. stavka 3. i članka 84. stavaka 2. i 3. ove Uredbe, sigurnosno-obavještajne agencije, u suradnji sa stranim sigurnosno-obavještajnim agencijama, neposredno razmjenjuju, prevoze ili pristupaju klasificiranim podacima operativno-analitičkog karaktera.

Razmjena osoba u sklopu projekata ili programa

Članak 86.

Kad se zaposlenik, koji posjeduje certifikat, premješta u pravnu osobu u drugoj državi, u sklopu istog programa ili projekta, pravna osoba, čiji se zaposlenik premješta, zatražit će od Ureda Vijeća za nacionalnu sigurnost dostavu potrebnih certifikata nadležnom sigurnosnom tijelu te države.
Zaposlenik iz stavka 1. ovog članka mora biti upoznat sa sigurnosnim standardima čije se provođenje zahtjeva pri međunarodnim posjetima.

VII. UPRAVLJANJE RIZIKOM INFORMACIJSKE SIGURNOSTI

Članak 87.

Državna tijela i pravne osobe iz članka 1. stavka 2. ove Uredbe, kad postupaju s klasificiranim podacima, dužne su upravljati rizikom informacijske sigurnosti.
Upravljanje rizikom informacijske sigurnosti sastoji se od trajnog procjenjivanja i obrade rizika, radi sprječavanja uništenja, otuđenja, gubitka i neovlaštenog pristupa klasificiranim podacima.

Procjenjivanje rizika informacijske sigurnosti

Članak 88.

Procjenjivanje rizika informacijske sigurnosti je sveobuhvatni proces vrednovanja rizika za klasificirane podatke.
Rezultati procjenjivanja rizika temelj su za odabir odgovarajućih mjera za zaštitu od rizika, sukladno prioritetima upravljanja rizicima.

Tijela i pravne osobe iz članka 1. stavka 2. ove Uredbe, dužne su voditi dnevnik procjenjivanja rizika, koji sadrži datum procjene, opis rizika, procjenu i vjerojatnost utjecaja pojedinog rizika, primijenjene sigurnosne mjere i izjavu o potrebnim sigurnosnim mjerama s određenim nositeljem i rokom provedbe.

Obrada rizika

Članak 89.

Obrada rizika je proces u kojem se za svaki procijenjeni rizik utvrđuje stupanj prihvatljivosti rizika, radi njegovog prihvaćanja, smanjenja ili izbjegavanja.

Članak 90.

Rizik se može prihvatiti ukoliko bi nastala šteta bila manja od štete koja bi nastala uslijed neprovođenja određene aktivnosti.
Smanjivanje rizika provodi se primjenom sigurnosnih mjera, radi sprječavanja uništenja, otuđenja, gubitka i neovlaštenog pristupa klasificiranim podacima.
Izbjegavanje rizika podrazumijeva poduzimanje organizacijskih mjera, u cilju izbjegavanja radnji koje bi mogle izazvati rizik.
Odluku o postupanju s preostalim rizikom, nakon obrade rizika, donosi čelnik tijela ili pravne osobe.

Članak 91.

Nakon donošenja odluke o obradi rizika, tijela i pravne osobe iz članka 1. stavka 2. ove Uredbe, obvezne su sačiniti plan obrade rizika u kojem se utvrđuje provođenje potrebnih mjera.

Članak 92.

Rezultati procjenjivanja i obrade rizika redovito se revidiraju, sukladno potrebama tijela ili pravne osobe, a radi nastalih unutarnjih ili vanjskih promjena.

VIII. NADZOR MJERA I STANDARDA INFORMACIJSKE SIGURNOSTI

Članak 93.

Nadzor nad provođenjem mjera i standarda informacijske sigurnosti u tijelima i pravnim osobama, koje koriste klasificirane i neklasificirane podatke, provode savjetnici za informacijsku sigurnost iz navedenih tijela i pravnih osoba.
Ured Vijeća za nacionalnu sigurnost provodi nadzor iz članka 30. stavka 1. Zakona o tajnosti podataka, u svim tijelima i pravnim osobama koja koriste klasificirane podatke stupnjeva tajnosti »Vrlo tajno«, »Tajno« i »Povjerljivo«, najmanje jednom u 2 godine, a u tijelima i pravnim osobama koja koriste klasificirane podatke stupnja tajnosti »Ograničeno« i neklasificirane podatke, najmanje jednom u 4 godine.
Sigurnosno-obavještajne agencije sudjeluju u nadzoru provedbe mjera informacijske sigurnosti u okviru poslova protuobavještajne zaštite, propisanih posebnim zakonom.

Članak 94.

Ured Vijeća za nacionalnu sigurnost izrađuje izvješće o provedenom nadzoru iz članka 92. stavka 1. i 2. ove Uredbe, i dostavlja ga u pisanom obliku čelniku tijela ili pravne osobe u kojoj je nadzor proveden.
Izvješće iz stavka 1. ovog članka sadrži i upute koje, u svrhu otklanjanja utvrđenih nedostataka i nepravilnosti, tijela i pravne osobe primjenjuju u zadanom roku.
Čelnik tijela ili pravne osobe iz stavka 1. ovog članka može se o izvješću očitovati Uredu Vijeća za nacionalnu sigurnost, u roku od 15 dana od dana primitka izvješća.
Ured Vijeća za nacionalnu sigurnost dužan je dati odgovor na očitovanje iz stavka 3. ovog članka, u roku od 30 dana od dana primitka očitovanja.

Članak 95.

Ured Vijeća za nacionalnu sigurnost kada, na temelju provedenog nadzora iz članka 92. stavka 1. i 2. ove Uredbe, utvrdi da se ne provode propisani sigurnosni standardi, izvijestit će, u pisanom obliku, nadležnu sigurnosno-obavještajnu agenciju, odnosno Zavod za sigurnost informacijskih sustava, koji će pokrenuti daljnje propisane radnje iz svog djelokruga.

IX. PRIJELAZNE I ZAVRŠNE ODREDBE

Članak 96.

Tijela i pravne osobe iz članka 1. stavka 2. ove Uredbe, dužna su donijeti sigurnosne mjere te uskladiti svoje poslovanje s odredbama ove Uredbe i pravilnika iz članaka 15. i 18. Zakona o informacijskoj sigurnosti, u roku od 12 mjeseci od donošenja ove Uredbe.

Članak 97.

Tijela i pravne osobe koje su, postupajući sukladno Zakonu o zaštiti tajnosti podataka (»Narodne novine«, broj 108/1996), uredile vlastite informacijske sustave, dužne su, u roku od 24 mjeseca od donošenja ove Uredbe, provesti sigurnosnu akreditaciju klasificiranih informacijskih sustava, u skladu s ovom Uredbom.
Tijela i pravne osobe iz stavka 1. ovog članka, do provedbe sigurnosne akreditacije klasificiranih informacijskih sustava, ne mogu u istima koristiti klasificirane podatke drugih država i međunarodnih organizacija s kojima je Republika Hrvatska potpisala međunarodni ugovor o uzajamnoj zaštiti klasificiranih podataka.

Članak 98.

Uvjeti propisani u članku 8. stavku 1. ove Uredbe, za informacijske sustave, moraju se ispuniti, u roku od 18 mjeseci od donošenja ove Uredbe.

Članak 99.

Ova Uredba stupa na snagu osmog dana od dana objave u »Narodnim novinama«.

Klasa: 650-05/08-02/01
Urbroj: 5030106-08-3
Zagreb, 18. travnja 2008.

Predsjednik
dr. sc. Ivo Sanader, v. r.

PRILOG

REPUBLIKA HRVATSKA
URED VIJEĆA ZA NACIONALNU SIGURNOST

Broj:

Certifikat poslovne sigurnosti pravne osobe

kojim se potvrđuje da je

Naziv pravne osobe: .....

Adresa: .....

MB: .....

---

sigurnosno provjeren za sklapanje klasificiranih ugovora stupnja tajnosti

STUPANJ TAJNOSTI

u skladu sa Zakonom o informacijskoj sigurnosti

Ured Vijeća za nacionalnu sigurnost potvrđuje da pravna osoba:

☐ ima akreditirani prostor za pohranu klasificiranih podataka stupnja tajnosti

STUPANJ TAJNOSTI

☐ nema akreditirani prostor za pohranu klasificiranih podataka

Datum izdavanja: ..... Vrijedi do: .....

Pečat

Predstojnik

_____