Na temelju članka 189. stavka 3. Zakona o mirovinskom osiguranju (Narodne novine, broj 157/2013) i članka 21. Statuta Hrvatskog zavoda za mirovinsko osiguranje (Narodne novine, broj 28/2014), a u vezi s člankom 106. stavkom 3. Zakona o mirovinskom osiguranju, Upravno vijeće Hrvatskog zavoda za mirovinsko osiguranje, na sjednici održanoj 18. prosinca 2014., donosi

PRAVILNIK
o zaštiti informacijskog sustava i tajnosti podataka Hrvatskog zavoda za mirovinsko osiguranje

I. OPĆE ODREDBE

Članak 1.

Ovim Pravilnikom utvrđuju se načini i mjere zaštite informacijskog sustava radi osiguravanja informacijske sigurnosti u Hrvatskom zavodu za mirovinsko osiguranje (u nastavku teksta: Zavod), tj. točnosti, cjelovitosti, dostupnosti i povjerljivosti podataka.

Ovim Pravilnikom utvrđuje se i koji se podaci u Zavodu smatraju poslovnom i profesionalnom tajnom te mjere za čuvanje, priopćavanje i korištenje tajnih podataka.

Članak 2.

Pojedini pojmovi u smislu ovoga Pravilnika imaju sljedeće značenje:

Informacijski sustav Zavoda je skup svih podataka, informacija i dokumentacije koje Zavod na temelju zakona prikuplja, stvara, pohranjuje, čuva, obrađuje i daje na korištenje, bez obzira na to u kojem su obliku i na kojem mediju ubilježeni. Informacijski sustav Zavoda obuhvaća i informatički sustav i ljudske resurse.

Informatički sustav Zavoda obuhvaća svu informatičku opremu (središnje računalo, poslužitelje, osobna računala i drugo), računalno-komunikacijsku mrežnu infrastrukturu, sistemski i aplikativni softver, baze podataka te računalne komponente (uključujući medije kao nositelje podataka) koje su u vlasništvu Zavoda ili su u upotrebi u Zavodu. Informatički sustav je podrška informacijskom sustavu.

Informacijska sigurnost je stanje povjerljivosti, cjelovitosti i raspoloživosti podataka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti.

Mjere informacijske sigurnosti su opća pravila zaštite informacijskog sustava na fizičkoj, tehničkoj ili organizacijskoj razini.

Podaci su svi podaci koji se nalaze ubilježeni na bilo kojem mediju i u bilo kojem obliku, čineći cjelokupan informacijski sklop pojedinog osiguranika, obveznika doprinosa, korisnika prava iz mirovinskog osiguranja i doplatka za djecu, odnosno fizičkih ili pravnih osoba čiji se podaci, na temelju propisa, prikupljaju, bilježe i obrađuju u Zavodu. Kao podaci, podrazumijevaju se i ostali podaci ubilježeni u Zavodu, kao što su osobni podaci o radnicima Zavoda, o imovini, podaci proizašli iz poslovnih procesa Zavoda i slično.

Osobni podatak je, u smislu propisa o zaštiti osobnih podataka, svaka informacija koja se odnosi na identificiranu fizičku osobu ili fizičku osobu koja se može identificirati izravno ili neizravno, posebno na osnovi identifikacijskog broja ili nekog drugog obilježja specifičnog za njezin fizički, psihološki, mentalni, gospodarski, kulturni ili socijalni identitet.

Zbirke osobnih podataka su evidencije koje Zavod vodi na temelju Zakona o mirovinskom osiguranju (matična evidencija) i drugih propisa, primjerice, propisa o radu, o doplatku za djecu itd., i koje sadrže osobne podatke osiguranika, korisnika prava iz mirovinskog osiguranja i doplatka za djecu, radnika Zavoda i drugih fizičkih osoba.

Profesionalnom tajnom smatraju se osobni podaci radnika, osiguranika, korisnika prava iz mirovinskog osiguranja i doplatka za djecu i drugih osoba koje saznaju radnici Zavoda u obavljanju svoga zanimanja i svojih poslova ili koje saznaju članovi Upravnog vijeća i drugih tijela Zavoda, a čije bi neovlašteno otkrivanje moglo štetiti interesu osobe na koju se podaci odnose ili članovima njene obitelji.

Poslovnom tajnom smatraju se podaci koji su zakonom, drugim propisom ili općim aktom Zavoda utvrđeni kao poslovna tajna, planovi i mjere fizičko-tehničke zaštite objekata i imovine te određene mjere informacijske sigurnosti, kao i podaci koje je Zavod kao poslovnu tajnu primio od drugih pravnih i fizičkih osoba ili tijela javne vlasti.

Dokumentacija podrazumijeva svu dokumentaciju koja je dio informacijskog sustava Zavoda, neovisno o tome je li zaprimljena ili je nastala u Zavodu.

Vlasnik poslovnog procesa je, u smislu ovoga Pravilnika, rukovoditelj sektora i samostalne ustrojstvene jedinice u Središnjoj službi te predstojnik područne ustrojstvene jedinice u čijem djelokrugu nastaje ili se koristi dokumentacija odnosno podaci.

Članak 3.

Za informacijsku sigurnost i za mjere zaštite informacijskog sustava u Zavodu, kao i za funkcioniranje sustava zaštite tajnosti podataka brinu se unutar svog djelokruga pomoćnici ravnatelja, rukovoditelji samostalnih ustrojstvenih jedinica u Središnjoj službi i predstojnici područnih ustrojstvenih jedinica, a odgovoran je ravnatelj Zavoda.

II. ZAŠTITA TAJNOSTI PODATAKA

Članak 4.

Tajnima se u Zavodu smatraju svi **osobni podaci** u zbirkama podataka koje Zavod vodi na osnovi propisa o mirovinskom osiguranju, doplatku za djecu, propisa o radu, uredskom poslovanju i na osnovi drugih propisa, sva dokumentacija u upravnim i neupravnim predmetima u Zavodu koja sadrži osobne podatke te pisana i usmena priopćenja ili informacije koje sadrže osobne podatke, a iznose se u radu tijela i stručne službe Zavoda.

Tajnim se smatraju i dokumenti i podaci koji su u Zavodu utvrđeni kao poslovna tajna (planovi i mjere fizičko-tehničke zaštite objekata i imovine Zavoda, ponude na natječaj i javno nadmetanje do objave rezultata i drugo).

Tajni su i podaci koji se kao poslovna ili profesionalna tajna saznaju od tijela javne vlasti i drugih pravnih i fizičkih osoba, klasificirani podaci, odnosno dokumentacija označena stupnjem tajnosti „vrlo tajno“, „tajno“, „povjerljivo“ ili „ograničeno“ i podaci koji su kao tajni utvrđeni zakonom ili drugim propisom.

Članak 5.

Podatke koji se smatraju tajnima dužni su čuvati svi radnici Zavoda, članovi Upravnog vijeća, ugovorni suradnici i druge osobe koje na bilo koji način i po bilo kojoj osnovi za njih saznaju u Zavodu te se ne smiju priopćavati, niti smiju biti dostupni neovlaštenim osobama.

Osobe iz stavka 1. ovoga članka dužne su čuvati tajnost podataka i nakon prestanka radnog odnosa, odnosno nakon razrješenja dužnosti članova upravnih i drugih tijela Zavoda, za sve vrijeme dok se podaci prema zakonu ili općem aktu Zavoda smatraju tajnom ili dok ih vlasnik podataka ne oslobodi dužnosti čuvanja tajnosti.

Članak 6.

Osobni podaci i dokumenti kojima raspolaže Zavod daju se samo ovlaštenim osobama, i to osiguraniku, korisniku prava iz mirovinskog osiguranja i doplatka za djecu i obvezniku uplate doprinosa, na temelju odgovarajućega zahtjeva.

Ostale osobe ovlaštene za pristup tajnim podacima isključivo su radnici Zavoda kojima su ti podaci potrebni za obavljanje njihovih poslova odnosno radnih zadataka, kao i ugovorni suradnici koji imaju pristup samo onim podacima i samo u opsegu koji im je potreban za izvršenje ugovorenog posla. Pristup tajnim podacima Zavoda mogu imati državna ili druga tijela te fizičke i pravne osobe koje su za to ovlaštene zakonom.

Osobni podaci koji se u Zavodu smatraju profesionalnom tajnom mogu se dati na korištenje primateljima (fizička ili pravna osoba, državno ili drugo tijelo) ako je to potrebno radi obavljanja poslova u okviru zakonom utvrđene djelatnosti primatelja, a na temelju pisanog zahtjeva koji mora sadržavati svrhu, vrstu podataka koji se traže i pravni temelj za korištenje, u skladu s propisima o zaštiti osobnih podatka.

Podatke iz članka 4. stavka 1. ovoga Pravilnika može dati na korištenje primateljima, isključivo pod uvjetima utvrđenim zakonom, ravnatelj Zavoda i, uz suglasnost službenika za zaštitu osobnih podataka, zamjenik ravnatelja, pomoćnici ravnatelja i predstojnici područnih ustrojstvenih jedinica, o čemu obvezno vode odgovarajuću evidenciju.

Podatke iz članka 4. stavka 2., koji su u Zavodu utvrđeni kao poslovna tajna, može dati na uvid, odnosno priopćiti, pod uvjetima utvrđenim zakonom, ravnatelj Zavoda ili osobe koje on za to ovlasti pisanom punomoći.

Podatke iz članka 4. stavka 3., koji se kao poslovna ili profesionalna tajna saznaju od tijela javne vlasti ili drugih pravnih i fizičkih osoba, klasificirane podatke odnosno dokumentaciju označenu stupnjem tajnosti „vrlo tajno“, „tajno“, „povjerljivo“ ili „ograničeno“ može, pod uvjetima utvrđenim zakonom i uz prethodnu pisanu suglasnost navedenih tijela, fizičkih ili pravnih osoba, dati ravnatelj Zavoda ili osobe koje on za to ovlasti pisanom punomoći.

Članak 7.

Zaštita **tajnosti** podataka osigurava se poduzimanjem fizičkih, tehničkih, organizacijskih i drugih mjera zaštite, kao što su, primjerice, ograničavanje pristupa, kontrola i evidentiranje korištenja te druge mjere, a odnose se na sve podatke odnosno dokumentaciju iz članka 4. ovoga Pravilnika, neovisno o tome u kojem se obliku i na kojem mediju nalaze.

Zaštita tajnosti podataka provodi se u ustrojstvenim jedinicama Zavoda u skladu s općim aktima Zavoda, a za provedbu mjera zaštite odgovorni su pomoćnici ravnatelja i rukovoditelji samostalnih ustrojstvenih jedinica u Središnjoj službi te predstojnici područnih ustrojstvenih jedinica Zavoda.

Povreda obveze čuvanja tajne

Članak 8.

Postupanjem protivno zakonu i odredbama ovoga Pravilnika i nepoštivanjem utvrđenih mjera zaštite tajnih podataka, radnik Zavoda čini osobito tešku povredu radne obveze i odgovara prema odredbama Zakona o radu za eventualnu za štetu uzrokovanu poslodavcu.

Prema članu Upravnog vijeća ili drugoj osobi koja nije radnik Zavoda, a koja otkrije tajne podatke ili na drugi način ne poštuje obvezu čuvanja tajnosti podataka, poduzet će se odgovarajuće mjere u skladu s propisima odnosno ugovorom i zahtijevat će se naknada eventualno nanesene štete.

Članak 9.

Na sjednicama tijela Zavoda, sastancima i drugim oblicima skupnog rada podaci koji se smatraju poslovnom ili profesionalnom tajnom mogu se priopćavati samo ako je takvo priopćavanje nužno za obavljanje poslova, pri čemu je osoba koja ih iznosi dužna upozoriti prisutne na obvezu čuvanja tajnosti podataka.

Članak 10.

Povredom obveze čuvanja tajne ne smatra se priopćenje koje osoba upoznata s tajnim podatkom iznese u prijavi kaznenog djela ili prekršaja nadležnom državnom tijelu.

III. MJERE SIGURNOSTI INFORMACIJSKOG SUSTAVA

Članak 11.

U Zavodu se obvezno provodi izobrazba radnika o informacijskoj sigurnosti i mogućim rizicima te njihovim obvezama i odgovornostima u vezi s tim.

Radnik Zavoda obvezno se pri zapošljavanju upoznaje s važećim propisima, općim aktima Zavoda, etičkim kodeksom, obvezom čuvanja tajnosti podataka i zaštitom informacijskog sustava Zavoda u cjelini, a posebno s dijelom koji se izravno odnosi na poslove njegovog radnog mjesta.

Radnici Zavoda pri zapošljavanju obvezno potpisuju izjavu o povjerljivosti.

Za provedbu odredaba ovoga članka odgovorni su neposredni rukovoditelj radnika i rukovoditelj unutarnje ustrojstvene jedinice nadležne za kadrovske poslove.

Članak 12.

U Zavodu se obvezno provodi stalna izobrazba i instruktaža radnika uputama za rad i na druge odgovarajuće načine.

Upute za rad, kao i opći i drugi akti Zavoda moraju se obvezno pohranjivati odnosno objavljivati u središnjoj bazi uputa i akata radi trajne dostupnosti svim radnicima Zavoda kojima su potrebni za obavljanje njihovih poslova.

Za provedbu odredaba iz stavka 1. ovoga članka odgovorni su, unutar svog djelokruga, rukovoditelji unutarnjih ustrojstvenih jedinica, a za provedbu odredaba iz stavka 2. ovoga članka odgovorni su donositelji (potpisnici) uputa i akata.

1. Opće mjere zaštite

Članak 13.

U Zavodu se provode sljedeće opće mjere zaštite, utvrđene zakonom, drugim propisima i općim aktima Zavoda:

- mjere fizičke i tehničke zaštite imovine i osoba, mjere zaštite od požara, zaštite arhivskog i registraturnog gradiva te zaštite na radu
- organizacijske mjere za osiguranje ažurnosti, točnosti i pravilnosti obavljanja poslova, kao i za sprječavanje neovlaštene izmjene dokumentacije i podataka te neovlaštenog korištenja informatičke opreme i mreže. Organizacijske mjere obuhvaćaju i sve radne postupke utvrđene uputama i standardima Zavoda, kao i mjere nadzora i kontrole.
- mjere za održavanje informatičkog sustava u funkciji koje se poduzimaju radi sprječavanja opasnosti od zastoja u radu cjelokupne ili dijela informatičke opreme, tj. sve aktivnosti i postupci kojima se osiguravaju tehnički i drugi uvjeti za rad, uključujući preventivne mjere i redovito održavanje informatičkog sustava.

2. Posebne mjere zaštite

Fizička sigurnost

Članak 14.

Prostorije pod posebnom zaštitom u Zavodu su:

1. prostorije u kojima je smješteno središnje računalo s pripadajućom informatičkom i komunikacijskom opremom (sistemska sala) i prostorije, kao i ormari u kojima su smješteni poslužitelji te pripadajuća informatička i komunikacijska oprema u središnjoj i područnim ustrojstvenim jedinicama
2. prostorije u kojima su arhivirane sigurnosne kopije podataka te sistemskog i aplikativnog softvera
3. prostorije u kojima je smještena dokumentacija za automatsku obradu podataka
4. prostorije u kojima je smještena poslovna dokumentacija koja omogućava rekonstrukciju poslovnih procesa i događaja
5. prostorije u kojima su smješteni spisi upravnih i neupravnih predmeta (pismohrane).

Odgovarajuće prostorije iz prethodnog stavka pisanim aktom određuje ravnatelj za Središnju službu, a predstojnici za područne ustrojstvene jedinice.

Članak 15.

Mjere zaštite za prostorije utvrđene člankom 14. ovoga Pravilnika su sljedeće:

- ulazak u prostorije dopušta se samo osobama koje su zaposlene u tim prostorijama i osobama koje imaju ovlaštenje za ulazak u te prostorije. Vanjski, ugovorni suradnici Zavoda, ovlašteni za ulazak u prostorije pod posebnom zaštitom, mogu ući i boraviti u navedenim prostorijama samo u nazočnosti nadležnog radnika Zavoda.
- obvezna nazočnost radnika u tim prostorijama odnosno zaključavanje prostorije za vrijeme radnog vremena i pri odlasku s posla te predaja ključa čuvarskoj službi
- obvezno zaključavanje ormara s informatičkom i komunikacijskom opremom, bez obzira na to nalaze li se u prostorijama ili na hodnicima
- zabrana iznošenja dokumentacije, informatičke opreme i nositelja podataka iz prostorije bez dopuštenja odgovorne osobe (uz obvezno vođenje evidencije), osim ako je to utvrđeno standardnim poslovnim procesom
- poimenično određivanje osoba odgovornih za održavanje odgovarajućih tehničkih uvjeta, čistoće i reda u prostoriji
- u prostorijama je zabranjeno audio i video snimanje
- instaliranje odgovarajuće opreme za protupožarnu zaštitu, što obuhvaća i automatski sustav za gašenje i vatrodojavu
- druge mjere fizičke ili tehničke zaštite koje u posebnim slučajevima određuje rukovoditelj nadležne unutarnje ustrojstvene jedinice.

Radi provedbe mjera iz ovoga članka obvezno se vodi popis svih radnika zaposlenih u prostorijama pod posebnom zaštitom, kao i osoba koje imaju ovlaštenje za ulazak u te prostorije, neovisno o tome jesu li zaposlenici ili vanjski suradnici Zavoda. Za vođenje i ažuriranje popisa odgovoran je rukovoditelj unutarnje ustrojstvene jedinice u sastavu koje se nalazi prostorija pod posebnom zaštitom.

Mjere iz stavka 1. alineje 1-4. ovoga članka neposredno provode radnici koji rade u tim prostorijama, a za nadzor nad provedbom tih mjera odgovorni su njihovi rukovoditelji. Za provedbu ostalih mjera iz stavka 1. ovoga članka odgovorni su načelnici odgovarajućih odjela u Sektoru za informatiku odnosno rukovoditelji nadležnih unutarnjih ustrojstvenih jedinica.

Članak 16.

Prostorije pod zaštitom u Zavodu su radne prostorije u kojima se nalazi ostala informatička i komunikacijska oprema (osobna računala, terminali i dr.) i radne prostorije u kojima su smješteni upravni i neupravni predmeti (osim pismohrana), kadrovski dosjei te prostorije u kojima je smješteno arhivsko gradivo Zavoda.

Mjere zaštite za ove prostorije su sljedeće:

- obvezno zaključavanje pri izlasku iz prostorije za vrijeme radnog vremena
- obvezno zaključavanje pri odlasku s posla
- obvezan nadzor čuvara i čuvanje ključeva za vrijeme i nakon radnog vremena
- zabrana iznošenja informatičke i komunikacijske opreme iz prostorije kao i dokumentacije izvan poslovne zgrade Zavoda bez dopuštenja odgovorne osobe (uz obvezno vođenje evidencije o tome), osim ako je to utvrđeno standardnim poslovnim procesom.

Mjere iz stavka 2. ovoga članka neposredno provode radnici zaposleni u tim prostorijama odnosno čuvari, a provedbu tih mjera, prema potrebi, kontroliraju njihovi rukovoditelji.

Članak 17.

Da bi se spriječio pristup neovlaštenih osoba opremi i dokumentaciji Zavoda, za stranke je potrebno osigurati primanje na šalterima. U situacijama gdje to nije moguće, primanje stranaka obavlja se, po mogućnosti, u posebnoj prostoriji u kojoj nije dostupna dokumentacija Zavoda i nije moguć pristup zaštićenim podacima.

Uvid u dokumentaciju upravnih predmeta strankama u postupku omogućava se uz obveznu nazočnost radnika Zavoda.

Sigurnost podataka

Članak 18.

U Zavodu se radi redovitog odvijanja poslovnih procesa poduzimaju odgovarajuće mjere za osiguranje zaštite, dostupnosti, cjelovitosti i točnosti podataka i dokumentacije od posebne važnosti.

U informatiziranim poslovnim procesima utvrđuju se i provode i posebne mjere zaštite, kao što su primjena propisane metodologije pri projektiranju i izvođenju, testiranje i verifikacija projekata prije predaje u produkciju, primjena utvrđenih pravila i standarda postupanja pri korištenju računalno-komunikacijskog sustava i drugo.

Članak 19.

Podaci i dokumentacija od posebne važnosti za Zavod su svi tajni podaci u zbirkama podataka i drugi podaci koji služe za odvijanje temeljnih i potpornih poslovnih procesa u Zavodu, projektna dokumentacija te sva poslovna dokumentacija koja omogućava rekonstrukciju poslovnih procesa i događaja, neovisno o mediju na kojem se nalazi.

Mjere zaštite za podatke i dokumentaciju od posebne važnosti su sljedeće:

- obvezno čuvanje i pohranjivanje papirne dokumentacije i drugih nositelja podataka u odgovarajućim, zaštićenim prostorijama ili u sefu
- čuvanje i pohranjivanje dokumentacije i podataka u odgovarajućem broju primjeraka
- osiguravanje pojedinih primjeraka dokumentacije i podataka kojima se omogućava rekonstrukcija poslovnih događaja na odgovarajućim nositeljima podataka (mikrofilm, diskovi, mikrofich, magnetske trake, diskete, CD, DVD itd.)
- obvezna izrada sigurnosnih kopija te čuvanje i pohranjivanje nositelja podataka u posebno zaštićenoj prostoriji u poslovnoj zgradi i na izdvojenoj lokaciji. Zaštićena prostorija na izdvojenoj lokaciji, u smislu ovoga Pravilnika, podrazumijeva poseban prostor udaljen od sjedišta Zavoda koji zadovoljava tehnološke i sigurnosne uvjete za čuvanje dokumentacije i nositelja podataka.
- obvezno čuvanje odgovarajućeg sistemskog i aplikativnog softvera onoliko dugo koliko se čuvaju sigurnosne kopije podataka ili pravodobno presnimavanje kopija na nove nositelje podataka.

Za provedbu mjera zaštite iz ovoga članka odgovorni su rukovoditelji nadležnih unutarnjih ustrojstvenih jedinica.

Sigurnosne kopije svoje službene dokumentacije na osobnom računalu izrađuje svaki radnik Zavoda.

Članak 20.

Dokumentacija klasificirana stupnjem tajnosti „vrlo tajno“, „tajno“, „povjerljivo“ i „ograničeno“ evidentira se u posebnoj evidenciji, a obvezno se pohranjuje u sef.

Članak 21.

Projektna dokumentacija se, kao dokumentacija od posebne važnosti, obvezno arhivira pri predaji programa u produkciju. Sastav projektne dokumentacije utvrđuje se posebnim općim aktom Zavoda o upravljanju projektima odnosno standardima za rad u automatskoj obradi podataka.

Općim aktom o projektiranju u Zavodu i standardima za rad u automatskoj obradi podataka utvrđuje se i metodologija rada koja pri projektiranju i izvođenju osigurava takve organizacijske postupke kojima se na djelotvoran način ostvaruje zaštita podataka te postupak verifikacije projekta pri predaji u produkciju.

Za svaku aplikaciju unutar koje se prikupljaju i koriste zakonom zaštićeni podaci projektnom dokumentacijom utvrđuju se mjere zaštite tih podataka.

Projektna dokumentacija iz stavka 1. ovoga članka čuva se najmanje pet godina nakon prestanka produkcije projekta ili aplikacije na koju se odnosi, odnosno dulje ako je tako utvrđeno Pravilnikom o zaštiti arhivskoga i registraturnoga gradiva.

Članak 22.

Uz dokumentaciju iz članka 19. stavka 1. ovoga Pravilnika, dokumentacijom od posebne važnosti za Zavod smatraju se i spisi upravnih i neupravnih predmeta (u vezi s ostvarivanjem prava iz mirovinskog osiguranja, doplatka za djecu, imovinskopravni predmeti, kadrovski predmeti i dosjei itd.) kao i sva ostala dokumentacija koja sadrži osobne podatke osiguranika, obveznika doprinosa, korisnika prava iz mirovinskog osiguranja i doplatka za djecu, radnika Zavoda i drugih fizičkih osoba, neovisno o obliku i mediju na kojem se nalaze.

Mjere zaštite za dokumentaciju iz prethodnog stavka su sljedeće:

- pristup dokumentaciji koja sadrži zakonom zaštićene podatke dopušta se samo ovlaštenim osobama
- dokumentacija u predmetima upravnog i neupravnog postupka kao registraturno gradivo Zavoda nakon isteka roka čuvanja mora se izlučiti i uništiti na način propisan zakonom odnosno općim aktom Zavoda o zaštiti arhivskog i registraturnoga gradiva
- ostala dokumentacija koja sadrži osobne podatke, kao što su razni ispisi iz baza podataka i slično, mora se uništiti strojnim rezanjem ili na drugi odgovarajući način (kontroliranom predajom u industrijsku preradu, uz odgovarajuće mjere osiguranja i evidenciju ili slično).

Mjeru zaštite iz alineje 1. stavka 2. ovoga članka neposredno provode radnici Zavoda, a za nadzor su odgovorni njihovi rukovoditelji. Ostale mjere iz ovoga članka provode rukovoditelji nadležnih unutarnjih ustrojstvenih jedinica.

Članak 23.

Kao mjera zaštite za osiguranje **točnosti podataka** obvezno se provodi utvrđivanje suodgovornosti radnika na određenim poslovima u Zavodu.

Mjera utvrđivanja suodgovornosti provodi se obveznom kontrolom:

- u pripremanju i donošenju rješenja o pravima iz MIO/INZ i DD u upravnom postupku, neovisno o načinu donošenja rješenja (ručno ili automatski)
- pri unosu podataka o stažu i plaći te drugim naknadama osiguranika, o iznosu mirovinskih primanja i doplatka za djecu i pri unosu podataka i storniranju iznosa u financijskim evidencijama
- pri unosu podataka o "ručno" obračunatim mirovinskim primanjima
- pri unosu podataka o ustegama od mirovina
- pri izmjeni projekata u produkciji
- u drugim važnim poslovima, prema odluci vlasnika poslovnog procesa odnosno u skladu s aktima Zavoda.

Članak 24.

Mjere zaštite za osiguranje točnosti ulaznih podataka u informatiziranim poslovnim procesima su sljedeće:

- podatke unosi isključivo ovlašteni radnik
- obveznu kontrolu unosa obavlja ovlašteni radnik (kontrola podataka i dokumentacije na osnovi koje se podaci unose)
- aplikativna i sustavna zaštita (primjerice, formalne i logičke kontrole, kontrolne svote, verifikacija unosa, dvostruki unos i slično)
- obvezno testiranje programa
- obvezna provjera izlazne dokumentacije.

Za provedbu mjera iz ovoga članka odgovoran je vlasnik poslovnog procesa.

Članak 25.

Mjere kontrole za pristup podacima u informatiziranim poslovnim procesima su sljedeće:

- pristup podacima dopušten je samo ovlaštenim radnicima
- praćenje i evidentiranje određenih aktivnosti na informatičkoj opremi odnosno računalno-komunikacijskoj mreži
- radnik smije koristiti samo svoju lozinku za pristup informatičkom sustavu Zavoda
- radnik mora zaštititi svoju lozinku
- pri dužem izbivanju s radnog mjesta (primjerice, pri odlasku na stanku, sastanak i slično), kao i pri odlasku s posla radnik se mora obvezno odjaviti iz aplikacija i sustava koje koristi
- pri odlasku s posla radnik mora obvezno isključiti informatičku opremu.

Za provedbu mjera iz alineje 1. do 2. stavka 1. ovoga članka odgovoran je Sektor za informatiku, a za mjere iz alineje 3. do 6. odgovorni su radnici Zavoda.

Članak 26.

Ovlaštenja za pristup, unos i kontrolu podataka dodjeljuju se radnicima Zavoda ovisno o njihovom radnom mjestu odnosno poslovima koje obavljaju.

Pomoćnik ravnatelja odgovarajućom odlukom utvrđuje pripadajuće skupine ovlaštenja za radna mjesta u svom sektoru, kao i za radna mjesta unutar nadležnosti sektora u područnim ustrojstvenim jedinicama.

Način i postupak dodjele, izmjene i ukidanja ovlaštenja radnicima odlukom propisuje ravnatelj Zavoda, a nadzor nad provedbom tog postupka obavlja unutarnja ustrojstvena jedinica nadležna za kontrolu i nadzor.

Članak 27.

Radnik Zavoda koji svoju lozinku da na korištenje neovlaštenoj osobi, u slučaju zlouporabe odgovara zbog povrede radne obveze i (su)odgovoran je za eventualnu štetu.

Radnik koji je namjerno ili zbog krajnje nepažnje unio ili dao pogrešne podatke ili je koristio tuđi identifikacijski podatak ili lozinku odgovara zbog teže povrede radne obveze, kao i za eventualnu štetu.

Sigurnost informatičkog sustava i opreme

Članak 28.

U Zavodu se obvezno primjenjuju mjere za zaštitu cjelovitosti softvera, podataka i informacija kojima se sprječava, otkriva i oporavlja od računalnih virusa i drugih štetnih programa i štiti informatička mreža od neovlaštenog pristupa.

Za određivanje i provedbu mjera iz prethodnog stavka odgovoran je Sektor za informatiku.

Ozbiljniji sigurnosni incidenti i poduzete aktivnosti obvezno se dokumentiraju radi sprječavanja budućih i poduzimanja eventualnih dodatnih mjera zaštite.

Radi zaštite informatičkog sustava, u Zavodu se smije koristiti samo softver koji je Zavod sam razvio, odgovarajući licencirani i provjereni programi ili programi koje je razvio vanjski poslovni partner na zahtjev i pod kontrolom Zavoda. Nove programe ili nove verzije programa mogu instalirati samo ovlaštene osobe Sektora za informatiku ili, uz nadzor nadležnog radnika Zavoda, ovlašteni djelatnici vanjskih ugovornih partnera koji obvezno potpisuju i izjavu o povjerljivosti.

U informatičku mrežu Zavoda ne smiju se, bez posebnog odobrenja Sektora za informatiku, priključivati udaljena i/ili privatna računala odnosno uređaji. O navedenom vodi se i posebna evidencija.

Sektor za informatiku vodi evidenciju softvera instaliranog u Zavodu, kao i svih korisničkih računa za pristup informatičko-komunikacijskoj mreži.

U Sektoru za informatiku vodi se i popis informatičke opreme s inventarnim brojem i zaduženjem.

Članak 29.

Nositelji podataka od posebne važnosti čuvaju se najmanje pet godina nakon prestanka produkcije pojedinog projekta, odnosno dulje, ako je tako utvrđeno općim aktom o zaštiti arhivskoga i registraturnoga gradiva.

Uz nositelje podataka obvezno se pohranjuju i odgovarajući sistemski i aplikativni programi, kao i eventualno potrebna oprema za učitavanje odnosno pristup podacima ili se podaci pravodobno presnimavaju na novije nositelje podataka.

Članak 30.

Posebnom sustavu zaštite podliježu i programi u sustavnim i aplikativnim bibliotekama, koji se nalaze na informatičkim medijima. Ovi programi čuvaju se najmanje pet godina nakon prestanka korištenja, odnosno dulje, ako je tako utvrđeno općim aktom o zaštiti arhivskoga i registraturnoga gradiva.

Članak 31.

U Zavodu se obvezno vodi evidencija svih korisničkih računa za pristup aplikacijama s pripadajućim podacima za identifikaciju.

Obvezno se vodi evidencija o dodijeljenim ovlaštenjima i, prema mogućnosti, svim izmjenama u ovlaštenjima koja sadrži najmanje sljedeće podatke:

- korisničko ime (userid)
- ime i prezime korisnika
- datum dodjele ovlaštenja
- datum oduzimanja ovlaštenja
- datum izmjene
- vrsta izmjene u ovlaštenjima.

Evidenciju iz ovoga članka vodi Sektor za informatiku u suradnji s unutarnjom ustrojstvenom jedinicom nadležnom za kadrovske poslove.

Članak 32.

Produkcijsko korištenje aplikacija obvezno se evidentira. Praćenje odnosno evidentiranje produkcijskog korištenja potrebno je na odgovarajući način osigurati i u nabavi gotovih aplikacija.

Evidentira se prvenstveno svako korištenje koje se odnosi na unos, verifikaciju (potvrđivanje), izmjenu ili brisanje podataka.

Evidencija iz stavka 1. ovoga članka obvezno sadrži:

- korisničko ime (userid)
- vrijeme i datum aktivnosti
- radni nalog za skupne obrade
- protokol o korištenju i pristupu podacima
- zapis o korisničkim aktivnostima (izmijenjeni i novi podaci).

Projektnom se dokumentacijom utvrđuje koji se podaci evidentiraju radi kontrole točnosti podataka i sprječavanja zlouporaba.

Podaci o aktivnosti odnosno korištenju aplikacija čuvaju se najmanje pet godina, odnosno dulje, ako je tako utvrđeno općim aktom o zaštiti arhivskoga i registraturnoga gradiva.

Članak 33.

Računalno-komunikacijski sustav i usluge dostupne putem tog sustava, a osobito internet i elektronička pošta, moraju se koristiti prvenstveno za obavljanje poslova Zavoda.

Radnik koji zlorabi informatički sustav ili usluge iz stavka 1. ovoga članka te prouzroči štetu imovini ili ugledu Zavoda odgovara zbog povrede radne obveze i za prouzročenu štetu.

Pod zlouporabom podrazumijeva se, primjerice:

- pristup, prijenos ili učitavanje podataka i instaliranje programa koji sigurnosno mogu ugroziti integritet mreže Zavoda i nelicenciranih programa
- pristup, prijenos ili učitavanje sadržaja diskriminirajuće, uznemiravajuće, ponižavajuće ili druge neprimjerene prirode koji su kao takvi utvrđeni posebnim propisima
- korištenje mreže i komunikacijskih alata u privatne komercijalne svrhe.

Zavod ima pravo kontrolirati korištenje informatičkog sustava i usluga iz stavka 1. ovoga članka i poduzimati tehničke mjere za sprječavanje zlouporaba. Odluku o primjeni tih mjera zaštite donosi ravnatelj Zavoda, a za provedbu mjera odgovoran je Sektor za informatiku.

Članak 34.

Podatke u informatičkom sustavu Zavoda mogu dodavati, brisati ili mijenjati samo osobe ovlaštene za to .

Ovlašteni radnici, odnosno ovlašteni korisnici računa su osobe koje sustav može identificirati na osnovi identifikacijskog podatka (lozinke) i pripadajuće autorizacije pristupa.

Način dodjeljivanja i izmjene lozinke te korištenje informatičke opreme i mreže utvrđuje Sektor za informatiku odgovarajućim uputama ili standardima za rad u uvjetima automatske obrade podataka.

Članak 35.

Mjere aplikativne i sustavne zaštite podataka i programa unutar informatičkog sustava Zavoda temelje se na sljedećim načelima:

1. dodavanje, brisanje i izmjena programa i podataka u informatičkom sustavu može se izvoditi samo na temelju valjanog pisanog naloga
2. sustavni i aplikativni programi koji bi mogli narušiti cjelovitost sustava moraju se pohraniti u posebnim, zaštićenim bibliotekama i zaštititi od neovlaštenog korištenja
3. pristup podacima treba omogućiti samo ovlaštenim radnicima one unutarnje ustrojstvene jedinice stručne službe Zavoda u čiji djelokrug spadaju ti podaci, odnosno drugim ovlaštenim radnicima
4. obvezno prijavljivanje i evidentiranje rada ovlaštenih radnika.

Provedba mjera iz prethodnog stavka obvezno se osigurava i projektnom dokumentacijom.

Članak 36.

Za ispravno funkcioniranje informatičkog sustava i tehničko održavanje informatičke opreme te sprječavanje opasnosti od nastupa dugotrajnijeg zastoja u radu odgovoran je Sektor za informatiku u Središnjoj službi.

Područne ustrojstvene jedinice stručne službe Zavoda u kojima je smještena informatička oprema odgovorne su za redovito održavanje te opreme u funkciji.

U slučaju zastoja ili problema u radu informatičke opreme, ustrojstvene jedinice stručne službe Zavoda odnosno unutarnje ustrojstvene jedinice dužne su zastoj ili kvar prijaviti Servisnom centru u Sektoru za informatiku.

Članak 37.

Mjerama zaštite osigurava se redovito održavanje informatičke opreme u funkciji, odnosno njezina djelotvorna zamjena u slučaju zastoja u radu.

Mjere zaštite prema stavku 1. ovoga članka su:

- donošenje plana za slučaj dugotrajnijeg zastoja u radu informatičkog sustava
- utvrđivanje i provedba standarda u radu i održavanju informatičke i pripadajuće opreme.

Članak 38.

Smatrat će se da je došlo do dugotrajnijeg zastoja u radu informatičkog sustava ako ključni dijelovi informatičkog sustava, kao što su središnje računalo i računalno-komunikacijski sustav te serveri Zavoda na kojima se nalazi dokumentacija potrebna za rad, zbog kvara ili drugog uzroka, nisu raspoloživi u vremenu za koje se može ocijeniti da će prouzročiti značajnije poremećaje u radu službe Zavoda.

Ocjenu da se radi o dugotrajnijem zastoju sustava donosi ravnatelj Zavoda.

Članak 39.

U slučaju izvanrednih okolnosti i dugotrajnijeg zastoja u radu informatičkog sustava postupa se prema planu koji donosi ravnatelj Zavoda.

Plan obvezno sadrži:

- unaprijed pripremljene rezervne lokacije na kojima će Zavod poslovati
- prioritete poslovnih aktivnosti koje će se odvijati na rezervnoj lokaciji
- prioritete obrade podataka koje se mogu obavljati na rezervnom sustavu
- točan redoslijed ponovnog uspostavljanja poslovnih aktivnosti Zavoda.

Način rada (odnosno obrade podataka) u slučaju dugotrajnijeg zastoja u radu informatičkog sustava Zavoda za svaku se pojedinačnu aplikaciju odnosno informatizirani poslovni proces utvrđuje projektnom dokumentacijom, u skladu s općim aktom o upravljanju projektima u Zavodu.

Članak 40.

Pomoćnik ravnatelja za informatiku utvrđuje standarde za rad u uvjetima automatske obrade podataka kojima se propisuju postupci u radu i na održavanju opreme.

Standardima iz stavka 1. ovoga članka odnosno odgovarajućim uputama propisuje se način rada i rukovanje opremom te upute za preventivno i redovito održavanje opreme.

Sigurnost suradnje i razmjene podataka

Članak 41.

U suradnji s fizičkim i pravnim osobama, državnim i drugim tijelima i ustanovama u Republici Hrvatskoj, kao i drugim državama i međunarodnim organizacijama, moraju se prepoznavati mogući rizici za informacijsku sigurnost Zavoda te poduzimati mjere zaštite za uklanjanje ili smanjivanje rizika.

Prije sklapanja ugovora o poslovnoj suradnji, na temelju kojeg bi pravna ili fizička osoba imala pristup tajnim podacima u Zavodu, potrebno je provesti provjeru druge ugovorne strane. Provjera obuhvaća utvrđivanje je li ta pravna ili fizička osoba registrirana za obavljanje potrebne djelatnosti i osigurava li dovoljno jamstava da će poduzeti odgovarajuće mjere zaštite osobnih i drugih tajnih podataka.

U ugovorima o poslovnoj suradnji, osobito ugovorima s izvršiteljima obrade osobnih podataka te ugovorima o nabavi usluga održavanja i drugih usluga potrebno je specificirati sigurnosne zahtjeve za pristup i postupanje s osobnim i drugim tajnim podacima.

Osoba odgovorna za praćenje izvršenja ugovora i rukovoditelj unutarnje ustrojstvene jedinice iz čijeg su djelokruga podaci poduzimaju sve mjere za zaštitu podataka tijekom izvršavanja ugovora. Ugovor treba sadržavati odredbe koje omogućavaju nadzor nad izvršenjem i kontrolu mjera zaštite podataka odnosno informacijskog sustava koje provodi druga ugovorna strana.

U slučaju kada je za sklapanje ugovora o suradnji prethodno nužno omogućiti pristup podacima, obvezno se sklapa ugovor ili sporazum o povjerljivosti kojim se druga strana obvezuje na poštivanje ili osiguravanje mjera zaštite informacijskog sustava. Pristup informacijskom sustavu Zavoda ne može se omogućiti prije početka važenja ugovora odnosno sporazuma o povjerljivosti.

Članak 42.

U slučajevima suradnje s državnim i drugim tijelima i ustanovama u Republici Hrvatskoj, kao i s drugim državama i međunarodnim organizacijama, koja se očituje u davanju na korištenje ili razmjeni osobnih podataka, primjenjuju se propisi o zaštiti osobnih podataka, osim ako posebnim zakonom nije drukčije određeno.

Mjere zaštite informacijskog sustava i tajnosti podataka potrebno je utvrditi u sporazumu ili ugovoru o davanju na korištenje ili o razmjeni osobnih podataka.

Članak 43.

U Središnjoj službi Zavoda obavljaju se poslovi zaštite informacijskog sustava odnosno usklađivanje, nadzor, izobrazba i koordinacija provedbe mjera i standarda informacijske sigurnosti.

Poslove iz stavka 1. ovoga članka obavlja savjetnik za informacijsku sigurnost kojeg odlukom imenuje ravnatelj Zavoda.

Savjetnik za informacijsku sigurnost je za svoj rad odgovoran neposredno ravnatelju Zavoda i najmanje dva puta godišnje podnosi izvještaj o stanju informacijske sigurnosti.

IV. ZAVRŠNE ODREDBE

Članak 44.

Odluke iz članka 26. stavka 2. i 3. i Plan iz članka 39. stavka 1. ovog Pravilnika donijet će se u roku od dva mjeseca od dana stupanja na snagu ovog Pravilnika.

Članak 45.

Na dan stupanja na snagu ovoga Pravilnika prestaje vrijediti Pravilnik o zaštiti tajnosti podataka i priopćavanju javnosti informacija o radu Hrvatskog zavoda za mirovinsko osiguranje, KLASA: 140-13/97-01/635 od 10. veljače 1997., KLASA 140-13/02-02/1324 od 6. veljače 2002. i KLASA: 140-13/02-02/2476 od 25. ožujka 2002. (pročišćeni tekst) i Pravilnik o zaštiti informatičke opreme, mreže, dokumentacije i podataka, KLASA: 140-13/04-02/3001 od 14. svibnja 2004.

Članak 46.

Ovaj Pravilnik stupa na snagu osmoga dana nakon objave na oglasnoj ploči u sjedištu Zavoda, A. Mihanovića 3 u Zagrebu.

KLASA: 041-01-14-02/11
URBROJ: 341-99-01/01-14-8
Zagreb, 18. prosinca 2014.

Predsjednica Upravnog vijeća
Hrvatskog zavoda za mirovinsko osiguranje

Mirjana Rađenović

O B R A Z L O Ž E N J E

U Zavodu se primjenjuje Pravilnik o zaštiti tajnosti podataka i priopćavanju javnosti informacija o radu Hrvatskog zavoda za mirovinsko osiguranje koji je donesen 10. veljače 1997., a izmijenjen je i dopunjen 6. veljače 2002. (pročišćeni tekst od 25. ožujka 2002.). U Zavodu se također primjenjuje Pravilnik o zaštiti informatičke opreme, mreže, dokumentacije i podataka koji je donesen 14. svibnja 2004.

Od donošenja navedenih pravilnika donesen je i izmijenjen čitav niz zakona, uredbi i podzakonskih propisa koji se (do)tiču područja zaštite podataka i sigurnosti informacijskog sustava, od kojih su najvažniji:

- Zakon o zaštiti osobnih podataka (Narodne novine, broj 103/2003, 118/2006, 41/2008, 130/2011 i 106/2012 – pročišćeni tekst)
- Zakon o tajnosti podataka (Narodne novine, broj 79/2007 i 86/2012)
- Zakon o informacijskoj sigurnosti (Narodne novine, broj 79/2007)

Od 1. siječnja 2014. na snazi je i novi Zakon o mirovinskom osiguranju (Narodne novine, broj 157/2013 – u nastavku: ZOMO) i novi Statut Hrvatskog zavoda za mirovinsko osiguranje (Narodne novine, broj 28/2014).

Osim na navedenim propisima, Nacrt prijedloga pravilnika temelji se i na dokumentu Strategija informacijske sigurnosti u Hrvatskom zavodu za mirovinsko osiguranje 2014.-2017., prema kojem je strateški cilj Zavoda uvođenje takvog sustava za upravljanje informacijskom sigurnošću koji će osigurati potpuniju zaštitu informacija kojima Zavod raspolaže, bez obzira na to u kojem se obliku nalaze.

Pri izradi Prijedloga pravilnika, koji sada objedinjuje područje zaštite tajnosti podataka i zaštite informacijskog sustava (uključujući informatički sustav), uzete su u obzir i preporuke unutarnje revizije u vezi s dodjelom ovlaštenja (zaštita podataka od neovlaštenog pristupa). Zavod nema klasificirane podatke, pa nije obvezan primijeniti sve mjere propisane za zaštitu takvih podataka, no one mjere koje su propisane ovim Prijedlogom pravilnika temelje se većinom na standardima HRN ISO/IEC 27001. Zavod u svom radu raspolaže pretežno osobnim podacima pa se primjenjuju mjere zaštite utvrđene propisima o zaštiti osobnih podataka.

Pravilnikom nije moguće obuhvatiti sve mjere zaštite, procedure i standarde koji se odnose na informacijsku sigurnost. Dio tzv. općih mjera zaštite u Zavodu propisan je drugim općim aktima (općim aktima o upravljanju projektima, o zaštiti arhivskog i registraturnog gradiva, zaštiti od požara, o radu i zaštiti na radu, o pravu na pristup informacijama itd.), a postoji i niz uputa za rad koje su već u primjeni ili će biti naknadno donesene.

Veći dio posebnih mjera zaštite informatičkog sustava preuzet je iz dosadašnjeg pravilnika jer je Zavod i do sada vrlo kvalitetno vodio brigu o sigurnosti svog informacijskog sustava, a najvažnije novosti su sljedeće:

- zaštita obuhvaća cijeli informacijski sustav, neovisno o mediju na kojem se podaci i dokumenti nalaze
- u prostorije pod posebnom zaštitom uključene su i pismohrane zbog velike količine dokumentacije koja se u njima pohranjuje
- propisane su i određene mjere za područje upravljanja ljudskim potencijalima odnosno izobrazbu radnika, a u vezi s tim je i obveza pohranjivanja odnosno objavljivanja uputa za rad i akata u središnjoj bazi Zavoda
- propisana je i sigurnost suradnje i razmjene podataka s drugima odnosno obveza ugrađivanja odgovarajućih klauzula u ugovore/sporazume

- propisana je obveza obavljanja poslova zaštite informacijskog sustava u Zavodu odnosno usklađivanje, nadzor, izobrazba i koordinacija provedbe mjera i standarda informacijske sigurnosti te izvještavanje o navedenom. U skladu s tim ustrojavaju se i poslovi savjetnika za informacijsku sigurnost kojeg imenuje ravnatelj Zavoda.

Novi pravilnik donosi Upravno vijeće Zavoda prema odredbi članka 189. stavka 3. ZOMO.

. - .