Na temelju članka 31. točke 3. Statuta Hrvatskog zavoda za mirovinsko osiguranje (Narodne novine, br. 28/14, 24/15, 73/19 i 147/20), a u vezi s člankom 24. stavkom 1. Zakona o informacijskoj sigurnosti (Narodne novine, br. 79/07), ravnatelj Hrvatskog zavoda za mirovinsko osiguranje donosi

PRAVILNIK
o informacijskoj sigurnosti u Hrvatskom zavodu za mirovinsko osiguranje

I. OPĆE ODREDBE

Članak 1.

Pravilnikom o informacijskoj sigurnosti u Hrvatskom zavodu za mirovinsko osiguranje (u daljnjem tekstu: Pravilnik) utvrđuje se okvir za upravljanje informacijskom sigurnošću, uloge i odgovornosti u sustavu upravljanja informacijskom sigurnošću, zahtjevi u području povjerljivosti, cjelovitosti i raspoloživosti informacijske imovine te najvažnije mjere zaštite informacijskog sustava u Hrvatskom zavodu za mirovinsko osiguranje (u daljnjem tekstu: Zavod).

Ovaj Pravilnik usklađen je sa zahtjevima međunarodne norme ISO/IEC 27001:2013.

Članak 2.

Svi ostali dokumenti informacijske sigurnosti u Zavodu moraju biti u skladu s ovim Pravilnikom.

Članak 3.

Ovaj Pravilnik odnosi se na sve poslovne procese i radnike Zavoda koji rukuju informacijskom imovinom radi zaštite povjerljivosti, cjelovitosti i raspoloživosti informacijske imovine.

Članak 4.

Akreditirani opseg Sustava upravljanja informacijskom sigurnošću utvrđuje se odlukom ravnatelja Zavoda. Na akreditirani opseg primjenjuju se načela i mjere propisane ovim Pravilnikom i međunarodnom normom ISO/IEC 27001:2013.

Članak 5.

Pojedini pojmovi u smislu ovog Pravilnika imaju sljedeće značenje:

1) **akreditirani opseg Sustava upravljanja informacijskom sigurnošću** obuhvaća unutarnje ustrojstvene jedinice Zavoda za koje je neovisnom provjerom utvrđena sukladnost sa zahtjevima međunarodne norme ISO 27001:2013.

2) **baza osobnih podataka** je evidencija koju Zavod vodi na temelju Zakona o mirovinskom osiguranju (matična evidencija) i drugih zakonskih propisa, primjerice, propisa o radu, o doplatku za djecu, nacionalnoj naknadi za starije osobe, i koja sadrži osobne podatke osiguranika, korisnika prava iz mirovinskog osiguranja i doplatka za djecu, korisnika prava na nacionalnu naknadu za starije osobe, radnika Zavoda i drugih fizičkih osoba.

3) **cjelovitost** je svojstvo informacije koje se odnosi na izvornost i potpunost, uz sprječavanje neovlaštene izmjene sadržaja.

4) **dokumentacija** je sva dokumentacija koja je dio informacijskog sustava Zavoda, neovisno o tome je li zaprimljena ili je nastala u Zavodu.

5) **incident informacijske sigurnosti** je događaj koji narušava povjerljivost, cjelovitost ili raspoloživost informacijske imovine, odnosno događaj (realizacija prijetnje zbog ranjivosti) koji uzrokuje kršenje zakonskih i drugih propisa, općih akata i uputa Zavoda u području informacijske sigurnosti.

6) **informacija** je skup podataka koji su ubilježeni na bilo kojem mediju i u bilo kojem obliku, čineći cjelokupan informacijski sklop o pojedinom osiguraniku, obvezniku doprinosa, korisniku prava iz mirovinskog osiguranja, doplatka za djecu i nacionalne naknade za starije osobe, radniku Zavoda, odnosno fizičkoj ili pravnoj osobi čiji se osobni i drugi podaci u Zavodu, na temelju zakona, prikupljaju, stvaraju, pohranjuju, obrađuju ili razmjenjuju. Informacija uključuje i ostale podatke u Zavodu, kao što su podaci o imovini, podaci koji proizlaze iz poslovnih procesa Zavoda (primjerice, projektna dokumentacija) i slično.

7) **informacijska imovina** su sve informacije kao i sva materijalna i nematerijalna sredstva koja služe za stvaranje, prikupljanje, obradu, pohranjivanje ili distribuciju informacija važnih u poslovnom procesu (primjerice, aplikacije, baze podataka, programski moduli, dokumentacija, ugovori, informatička oprema, dijelovi infrastrukture, pomoćne usluge, uredski prostori).

8) **informacijska sigurnost** je stanje povjerljivosti, cjelovitosti i raspoloživosti informacija, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda. Informacijska sigurnost je širi pojam od informatičke sigurnosti i odnosi se na zaštitu informacija bez obzira na medij na kojem se nalaze, tj. nalaze li se u fizičkom ili elektroničkom obliku.

9) **informacijski sustav Zavoda** je skup svih informacija i dokumentacije koje Zavod na temelju zakona i drugih propisa 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 informacijsku imovinu i ljudske resurse.

10) **informatički sustav Zavoda** je skup cjelokupne informatičke opreme (središnje računalo, poslužitelji, osobna računala i drugo), računalno-komunikacijske mrežne

infrastrukture, sistemskog i aplikativnog softvera, baza podataka te računalnih komponenti (uključujući medije kao nositelje informacija) koji su u vlasništvu Zavoda ili su u upotrebi u Zavodu. Informatički sustav je podrška informacijskom sustavu.

11) **korisnik sustava** je svaka osoba koja koristi informatički sustav u vlasništvu Zavoda (primjerice, radnici Zavoda, vanjski pružatelji usluga).

12) **kriptografske kontrole** napredni su oblici zaštite informacija od neovlaštenog pristupa ili presretanja kojima se osigurava da su pohranjene informacije ili informacije tijekom prijenosa nečitljive neovlaštenim osobama. Ovim kontrolama osiguravaju se različiti ciljevi kao što su povjerljivost, cjelovitost i autentičnost informacija.

13) **mjere informacijske sigurnosti** su opća pravila zaštite informacijskog sustava na fizičkoj, tehničkoj, organizacijskoj i kadrovskoj razini.

14) **norma ISO/IEC 27001:2013** je međunarodna norma ustanovljena da bi utvrdila zahtjeve za uspostavljanje, uvođenje, održavanje i trajno poboljšanje sustava upravljanja informacijskom sigurnošću.

15) **nositelj informacija** je medij na kojem je određena informacija pohranjena, primjerice mikrofilm, papir, CD/DVD, čvrsti disk i slično.

16) **osobni podaci** su u smislu propisa o zaštiti osobnih podataka svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi („ispitanik"); pojedinac čiji se identitet može utvrditi je osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca.

17) **plan kontinuiteta poslovanja** je skup dokumentiranih procedura za odgovor, oporavak, nastavak i vraćanje Zavoda u stanje redovitog rada.

18) **poslovna tajna** su, prema odredbama Statuta Zavoda, informacije koje su zakonom, drugim propisom ili općim aktom Zavoda utvrđene kao poslovna tajna, planovi i mjere fizičko-tehničke zaštite objekata i imovine te određene mjere informacijske sigurnosti, kao i informacije koje je Zavod kao poslovnu tajnu primio od drugih pravnih i fizičkih osoba ili tijela javne vlasti.

19) **poslovni proces** je povezani skup aktivnosti i mjera koji se provodi radi ostvarenja mjerljivog cilja organizacije i troši resurse pretvarajući ih u specifične proizvode ili usluge.

20) **povjerljivost** je svojstvo informacije da nije dostupna neovlaštenim osobama, entitetima ili procesima.

21) **povreda osobnih podataka** je kršenje sigurnosti osobnih podataka koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani.

22) **profesionalna tajna** su, prema odredbama Statuta Zavoda, osobni podaci radnika, osiguranika i korisnika prava iz mirovinskog osiguranja i doplatka za djecu, korisnika prava na nacionalnu naknadu za starije osobe 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 bilo protivno propisima o zaštiti osobnih podataka.

23) **ranjivost informacijskog sustava** je slabost informacijske imovine ili skupine informacijske imovine koju jedna ili više prijetnji mogu iskoristiti (slaba točka ili kritična točka unutar sustava) i čije iskorištavanje može prouzročiti štetu na sustavu.

24) **raspoloživost** je svojstvo informacije da je dostupna i upotrebljiva na zahtjev ovlaštenog korisnika.

25) **registar informacijske imovine** je jedinstveni popis informacijske imovine koju treba adekvatno zaštititi od prijetnji i ranjivosti i na kojoj treba provesti procjenu rizika.

26) **rizik** je incident ili pojava koja nastaje iz unutarnjih ili vanjskih izvora, a koji može nepovoljno utjecati na ostvarenje ciljeva informacijske sigurnosti. Rizikom se smatraju i neiskorištene prilike ili mogućnosti za poboljšanje poslovanja.

27) **sigurnosni događaj** je stanje sustava, usluge ili mreže koje upućuje na moguću povredu politike informacijske sigurnosti, neuspjeh zaštite ili do tada nepoznate okolnosti koje mogu biti važne za informacijsku sigurnost.

28) **upravljanje kontinuitetom poslovanja** je proces koji omogućava Zavodu učinkovit odgovor i oporavak ključnih poslovnih procesa i usluga u slučaju njihovog iznenadnog i neželjenog prekida.

29) **vanjski pružatelj usluga** je fizička ili pravna osoba koja je u ugovornom odnosu sa Zavodom radi obavljanja funkcija ili dijela funkcije ili za Zavod dobavlja određene resurse, znanja ili kompetencije.

30) **vlasnik informatičkog sustava** je osoba odgovorna za organizaciju i ispravno funkcioniranje informatičkog sustava podržanog IT tehnologijom, a u skladu s usuglašenim zahtjevima s vlasnikom poslovnog procesa. Vlasnik informatičkog sustava odgovoran je za upravljanje operativnim radom informatičkog sustava.

31) **vlasnik poslovnog procesa** je rukovoditelj sektora ili samostalne ustrojstvene jedinice u Središnjoj službi te predstojnik područne ustrojstvene jedinice u čijem djelokrugu nastaje, prikuplja se ili koristi dokumentacija odnosno informacije. Odgovoran je za informacije i funkcioniranje informacijskog sustava.

II. ULOGE I ODGOVORNOSTI

Članak 6.

Odgovorne osobe i odgovornosti za informacijsku sigurnost u Zavodu određuju se s obzirom na radna mjesta te znanja i vještine koje su potrebne za ispunjenje zahtjeva za pravilno funkcioniranje pojedinog područja informacijske sigurnosti.

Članak 7.

Ravnatelj Zavoda odgovoran je za uspostavu i razvoj učinkovitog i djelotvornog sustava upravljanja informacijskom sigurnošću u poslovanju Zavoda te u vezi s tim:

- određuje ciljeve informacijske sigurnosti
- osigurava resurse potrebne za upravljanje informacijskom sigurnošću
- osigurava izvršavanje ciljeva upravljanja informacijskom sigurnošću
- motivira svojim aktivnostima podizanje razine informacijske sigurnosti u Zavodu.

Članak 8.

Predstojnik Ureda za poslovno-informacijsku sigurnost, kontrolu i nadzor odgovoran je za održavanje i trajno poboljšavanje djelotvornog sustava upravljanja informacijskom sigurnošću te u vezi s tim:

- osigurava da upravljanje informacijskom sigurnošću bude u skladu s poslovnim potrebama i strategijom, regulatornim zahtjevima i dobrim praksama
- osigurava da svi radnici Zavoda budu upoznati s ovim Pravilnikom
- predlaže implementaciju mjera za ublažavanje rizika nad informacijskom imovinom
- nadzire provedbu, djelotvornost i učinkovitost propisanih mjera i kontrola informacijske sigurnosti
- vodi jedinstveni registar informacijske imovine Zavoda po poslovnim procesima i odgovoran je za njegovu povjerljivost, cjelovitost i raspoloživost
- koordinira proces procjene rizika informacijske imovine i prati realizaciju mjera za obradu rizika
- u slučaju incidenata informacijske sigurnosti, organizira provedbu analize uzroka incidenta uvidom u informacijski sustav Zavoda i u druge izvore te o rezultatima podnosi izvještaj ravnatelju.

Članak 9.

Savjetnik za informacijsku sigurnost imenuje se odlukom ravnatelja, a odgovoran je za poslove zaštite informacijskog sustava, odnosno usklađivanje, nadzor, edukaciju i koordinaciju provedbe mjera i standarda informacijske sigurnosti u Zavodu.

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

Članak 10.

Pomoćnici ravnatelja, rukovoditelji samostalnih ustrojstvenih jedinica u Središnjoj službi te predstojnici područnih ustrojstvenih jedinica brinu se o provedbi mjera zaštite u poslovnim procesima koje su ovlašteni organizirati. Na temelju funkcionalne nadležnosti odgovorni su za:

- podršku i primjenu sustava upravljanja informacijskom sigurnošću u svom djelokrugu
- osiguranje provedbe svih mjera zaštite u svom djelokrugu, propisanih aktima informacijske sigurnosti koje uključuju, ali nisu ograničene ovim Pravilnikom, upute, procedure i standarde Zavoda
- provedbu kontinuirane procjene rizika informacijske sigurnosti unutar svojeg djelokruga kao i redovno održavanje registra informacijske imovine prema zahtjevima cjelovitosti, raspoloživost i povjerljivosti
- organiziranje poslova na siguran način i kontinuirano upoznavanje i osvještavanje radnika o prihvatljivim i sigurnim načinima rada te nadzor nad radom radnika
- sudjelovanje u razvoju informacijskog sustava unutar svojeg djelokruga poslova i koordinaciji provedbe mjera zaštite temeljenih na procjeni rizika informacijske sigurnosti
- suradnju s Uredom za poslovno-informacijsku sigurnost, kontrolu i nadzor u provedbi, poboljšanju i predlaganju novih mjera zaštite i izvještavanju o statusu aktivnosti i stanju informacijske sigurnosti.

Članak 11.

Svi radnici osobno su odgovorni za poznavanje i provedbu propisanih mjera i kontrola te suradnju u rješavanju incidenata informacijske sigurnosti u okviru svojih poslovno definiranih odgovornosti prema važećim internim aktima o unutarnjem ustrojstvu i sistematizaciji radnih mjesta u Zavodu.

Članak 12.

Vanjski pružatelji usluga odgovorni su za uspostavu i održavanje odgovarajuće razine informacijske sigurnosti pri pružanju usluga i proizvoda Zavodu, u skladu sa sklopljenim ugovorima sa Zavodom i važećim propisima.

III. ZAŠTITA POVJERLJIVOSTI, CJELOVITOSTI I RASPOLOŽIVOSTI INFORMACIJA

Povjerljivost

Članak 13.

Prema razini povjerljivosti, informacije u Zavodu klasificiraju se kao javne, poslovno važne i tajne.

Članak 14.

Javne informacije su informacije koje Zavod javno objavljuje, koje se koriste unutar Zavoda te one kojima je u određenim uvjetima omogućen pristup trećim osobama.

Članak 15.

Poslovno važne informacije su informacije koje nisu tajne, ali su bitne za kontinuitet poslovanja Zavoda, odnosno za rekonstrukciju poslovnih procesa i događaja, a koriste ih radnici Zavoda u skladu s dodijeljenim ovlaštenjima.

Članak 16.

Tajne informacije su informacije koje su Statutom Zavoda propisane kao profesionalna ili poslovna tajna, osobni podaci i tajne ili klasificirane informacije zaprimljene u Zavodu, a koriste ih radnici Zavoda u skladu s dodijeljenim ovlaštenjima.

Informacije klasificirane stupnjem tajnosti primljene izvana koristi ograničeni broj radnika Zavoda, u skladu s propisima iz područja informacijske sigurnosti i tajnosti podataka.

Članak 17.

Kada informacijska imovina sadrži informacije različitih klasifikacijskih razina povjerljivosti, primjenjuje se najviša razina klasifikacije.

Članak 18.

Tajnima se u Zavodu smatraju svi osobni podaci u bazama podataka koje Zavod vodi i obrađuje na osnovi propisa o mirovinskom osiguranju, doplatku za djecu, nacionalnoj naknadi za starije osobe, 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 dokumenti i informacije koje su u Zavodu utvrđene kao poslovna tajna (primjerice, planovi i mjere fizičko-tehničke zaštite objekata i imovine Zavoda, ponude na natječaj i javno nadmetanje do objave rezultata, mjere informacijske sigurnosti).

Tajne su i informacije koje se kao poslovna ili profesionalna tajna saznaju od tijela javne vlasti i drugih pravnih i fizičkih osoba, klasificirane informacije, odnosno dokumentacija označena stupnjem tajnosti „vrlo tajno", „tajno", „povjerljivo" ili „ograničeno" i informacije koje su kao tajne utvrđene zakonom ili drugim propisom.

Članak 19.

Informacije koje se smatraju tajnima dužni su čuvati svi radnici Zavoda, članovi Upravnog vijeća, vanjski pružatelji usluga i druge osobe koje na bilo koji način i po bilo kojoj osnovi za njih saznaju u Zavodu te se ne smiju priopćavati i ne smiju biti dostupne neovlaštenim osobama.

Osobe iz stavka 1. ovoga članka dužne su čuvati tajnost informacija i nakon prestanka radnog ili ugovornog odnosa, odnosno nakon razrješenja dužnosti članova upravnih i drugih tijela

Zavoda, za sve vrijeme dok se informacije prema zakonu ili općem aktu Zavoda smatraju tajnom ili dok ih vlasnik informacija ne oslobodi dužnosti čuvanja tajnosti.

Na sjednicama tijela Zavoda, sastancima i drugim oblicima skupnog rada informacije koje 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 informacija.

Članak 20.

Osobe ovlaštene za pristup tajnim informacijama su radnici Zavoda kojima su te informacije potrebne za obavljanje njihovih poslova odnosno radnih zadataka, kao i vanjski pružatelji usluga koji imaju pristup samo onim informacijama i samo u opsegu koji im je potreban za izvršenje ugovorenog posla.

Pristup tajnim informacijama Zavoda mogu imati državna ili druga tijela te druge pravne i fizičke osobe koje su za to ovlaštene zakonom, ako je to potrebno radi obavljanja poslova u okviru zakonom utvrđene djelatnosti primatelja, a na temelju pisanog zahtjeva koji mora sadržavati svrhu, vrstu informacija koje se traže i pravni temelj za korištenje.

Informacije koje su u Zavodu utvrđene kao poslovna tajna može dati na uvid, odnosno priopćiti, u uvjetima utvrđenim zakonom, ravnatelj Zavoda ili osobe koje on za to ovlasti.

Informacije koje se kao poslovna ili profesionalna tajna saznaju od drugih tijela javne vlasti ili drugih pravnih i fizičkih osoba, klasificirane informacije odnosno dokumentaciju označenu stupnjem tajnosti „vrlo tajno", „tajno", „povjerljivo" ili „ograničeno" može, u uvjetima utvrđenim zakonom i uz prethodnu pisanu suglasnost navedenih tijela ili drugih pravnih i fizičkih osoba, dati ravnatelj Zavoda ili osobe koje on za to ovlasti.

Članak 21.

Zaštita povjerljivosti informacija 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 informacije, neovisno o tome u kojem se obliku i na kojem mediju nalaze.

Cjelovitost

Članak 22.

Razine cjelovitosti informacija u Zavodu određuju se kao standardna ili kao visoka s obzirom na visinu moguće štete Zavodu zbog neovlaštenih izmjena ili brisanja informacija.

Članak 23.

Standardna razina cjelovitosti odnosi se na one informacije koje neovlaštenim izmjenama ili brisanjem neće stvoriti značajnu pravnu, financijsku ili reputacijsku štetu Zavodu.

Članak 24.

Visoka razina cjelovitosti odnosi se na one informacije koje ne smiju sadržavati pogreške (primjerice, matični podaci osiguranika) odnosno u slučajevima u kojima je zbog pogrešaka ili odluka temeljenih na pogrešnim informacijama moguća značajna pravna, financijska ili reputacijska šteta Zavodu.

Članak 25.

Kada informacijska imovina sadrži informacije različitih klasifikacijskih razina cjelovitosti, na cijelu informacijsku imovinu uvijek se primjenjuje najviša razina klasifikacije.

Raspoloživost

Članak 26.

Razine raspoloživosti informacija u Zavodu određuju se kao standardna ili kao visoka, a procjenjuju se s obzirom na njihovu dostupnost u trenutku kada su one potrebne, odnosno u normalnim ili izvanrednim uvjetima te s obzirom na štetu koja može nastati ako određena informacijska imovina ili informacije u danom trenutku nisu dostupne ili su neupotrebljive.

Članak 27.

Standardna razina raspoloživosti odnosi se na one informacije za koje je ciljano vrijeme oporavka više od 24 sata (jedan dan).

Članak 28.

Visoka razina raspoloživosti odnosi se na one informacije za koje je ciljano vrijeme oporavka manje ili jednako 24 sata (jedan dan).

Članak 29.

Ako informacijska imovina sadrži informacije različitih klasifikacijskih razina raspoloživosti, na cijelu informacijsku imovinu uvijek se primjenjuje najviša razina klasifikacije.

Članak 30.

Klasifikacija informacijske imovine prema povjerljivosti, cjelovitosti i raspoloživosti detaljnije se uređuje uputama koje donosi ravnatelj Zavoda.

IV. MJERE ZAŠTITE INFORMACIJSKOG SUSTAVA

Procjena rizika

Članak 31.

Zaštita informacijskog sustava temelji se na upravljanju rizicima.

Upravljanje rizicima detaljnije se uređuje uputama o upravljanju rizicima koje donosi ravnatelj Zavoda.

Članak 32.

Vlasnici poslovnih procesa upravljaju rizicima u svojim ustrojstvenim jedinicama te najmanje jedanput godišnje:

- ažuriraju popis (registar) informacijske imovine
- procjenjuju rizike i analiziraju utjecaj rizika na poslovanje
- odlučuju o mjerama za uklanjanje ili smanjenje rizika.

Vlasnici poslovnih procesa organiziraju izvanrednu provedbu aktivnosti navedenih u stavku 1. ovoga članka nakon znatnih incidenata, aktivacije planova kontinuiteta poslovanja i/ili kriznog upravljanja, uočenih većih nesukladnosti te značajnijih izmjena poslovnih procesa ili tehnologija. Prema potrebi, u ove se aktivnosti uključuje i savjetnik za informacijsku sigurnost.

Na temelju informacija koje dostavljaju vlasnici poslovnih procesa, Ured za poslovno-informacijsku sigurnost, kontrolu i nadzor izrađuje godišnji izvještaj o aktivnostima koji uključuje najvažnije rizike informacijske sigurnosti, rezultate analize utjecaja na poslovanje, status implementacije i provedbu mjera za obradu rizika informacijske sigurnosti te relevantne trendove i preporuke na razini Zavoda.

Članak 33.

U identifikaciji mogućih rizika i mjera obrade rizika, Zavod surađuje s državnim, javnim i drugim tijelima i ustanovama u Republici Hrvatskoj, drugim pravnim i fizičkim osobama u Republici Hrvatskoj te drugim državama i međunarodnim organizacijama.

Članak 34.

Mjere zaštite informacijskog sustava trebaju biti razmjerne klasifikaciji informacijske imovine koje se određuju u skladu s rezultatima procjene rizika i analizom utjecaja na poslovanje.

Količina, opseg i doseg kontrola informacijske sigurnosti na određenoj informacijskoj imovini ovisi o negativnom financijskom, reputacijskom i pravnom učinku na povjerljivost, cjelovitost i raspoloživost.

Sigurnost u upravljanju projektima

Članak 35.

Upravljanje informacijskom sigurnošću obvezan je element upravljanja projektima, neovisno o vrsti i veličini projekta.

Odgovornost za informacijsku sigurnost u provedbi projekata propisuje se općim aktom o provedbi projekata u Zavodu.

Sigurnost u upravljanju projektima uključuje procjenu rizika tijekom rada na projektu, ažuriranje relevantnih registara informacijske imovine, donošenje mjera upravljanja rizicima i druge aktivnosti, u skladu s općim aktom o provedbi projekata u Zavodu.

Upravljanje prijenosnim uređajima

Članak 36.

Radnik zadužen prijenosnim uređajem upravlja rizicima i poduzima sigurnosne mjere radi zaštite i sprječavanja kompromitiranja pohranjenih informacija.

Na prijenosnim računalima instalira se cjelokupan korisnički softver potreban za obavljanje uobičajenih poslovnih zadataka i postupaka, kao i zaštita od zlođudnog softvera koja se redovito ažurira.

Članak 37.

Zaduženo prijenosno računalo radnici su obvezni jednom unutar dva mjeseca donijeti na radno mjesto te ga čitav radni dan ostaviti uključenog u informatičku mrežu Zavoda kako bi se izvršilo pozadinsko sistemsko ažuriranje softvera i procedura.

Radnicima nije dopušteno i ne smije biti omogućeno samostalno instaliranje softvera na prijenosne uređaje, osim u slučaju prethodno odobrenog opravdanog poslovnog zahtjeva.

Na razini Zavoda onemogućava se pristup nesigurnim i poslovno neprimjerenim web-aplikacijama i servisima.

Rad na daljinu

Članak 38.

U Zavodu je dopušten rad na daljinu samo pod uvjetom da su primijenjene sve sigurnosne kontrole utvrđene ovim Pravilnikom.

Radnicima Zavoda se na temelju obrazloženog zahtjeva dostavljenog Sektoru za informatiku omogućava rad na daljinu dodjeljivanjem prava preko imeničnog servisa.

Prostor u kojem se obavlja rad na daljinu mora biti siguran i zaštićen od krađe uređaja i neovlaštenog pristupa informacijama kojima se može pristupati putem tih uređaja.

Konfiguraciju rada na daljinu provodi Sektor za informatiku.

Članak 39.

Rad na daljinu vanjskim pružateljima usluga Zavodu, s pripadajućim pravima pristupa, odobrava pomoćnik ravnatelja za informatiku.

Formalni zahtjev koji se dostavlja pomoćniku ravnatelja za informatiku podnosi se na tiskanici zahtjeva za pristup informatičkom sustavu koju utvrđuje Sektor za informatiku i koja sadrži podatke o podnositelju zahtjeva, trajanju pristupa i razlozima pristupa.

Sigurnost ljudskih resursa

Članak 40.

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 i tijekom rada u Zavodu upoznaje s važećim propisima, općim aktima i uputama za rad Zavoda, obvezom čuvanja informacija, zaštitom informacijskog sustava Zavoda u cjelini, a posebno sa zahtjevima koji se izravno odnose na poslove njegovog radnog mjesta.

Upute za rad, kao i opći i drugi akti Zavoda moraju se obvezno pohranjivati odnosno objavljivati tako da budu trajno dostupni svim radnicima Zavoda kojima su potrebni za obavljanje njihovih poslova.

Članak 41.

Radnici Zavoda pri zapošljavanju potpisuju ugovor o radu koji mora sadržavati odredbe koje se odnose na obvezu čuvanja povjerljivosti, cjelovitosti i raspoloživosti informacija.

Članak 42.

Posebnim općim aktima Zavoda propisuju se procesi vezani uz sigurnost ljudskih resursa, postupak odabira radnika pri zapošljavanju u Zavodu, kontrole i mjere u slučaju promjene radnog mjesta ili odlaska radnika iz Zavoda (primjerice, povrat opreme) kao i disciplinski postupci.

Upravljanje imovinom

Članak 43.

Zavod vodi i održava ažurnima registre informacijske imovine unutarnjih ustrojstvenih jedinica i utvrđuje prikladne kontrole za njihovu zaštitu, u skladu s procjenom rizika, analizom utjecaja na poslovanje i klasifikacijskim oznakama imovine.

Postupanje s informacijskom imovinom mora se provoditi na siguran način.

Članak 44.

Procesi i kontrole vezane uz upravljanje informacijskom imovinom detaljnije se uređuju uputama koje donosi ravnatelj Zavoda.

Kontrola pristupa

Članak 45.

Mjerama kontrole pristupa štiti se informacijska imovina tako da se nadziru sve ulazne i izlazne točke informacijskog sustava.

Mjerama fizičke i logičke zaštite štiti se osjetljiva imovina od neovlaštenog korisničkog pristupa.

Članak 46.

Pravo na pristup informacijskom sustavu, odnosno dijelovima informacijskog sustava Zavoda dodjeljuje se u skladu s poslovnim potrebama i zahtjevima sigurnosti.

Ovlaštenja za pristup informacijskom sustavu ne smiju biti veća od onih koja su dovoljna za obavljanje poslova i zadataka iz pripadajućeg poslovnog procesa i moraju se provjeravati najmanje jedanput godišnje.

Upravljanje identitetom korisnika sustava, ovlaštenjima za pristup i autorizacijama detaljnije se uređuje uputama koje donosi ravnatelj Zavoda.

Korištenje interneta i elektroničke pošte

Članak 47.

Radi zaštite povjerljivosti, cjelovitosti i raspoloživosti informacijske imovine Zavoda te osiguranja kontinuiteta poslovnih procesa, korištenje interneta i službene elektroničke pošte štiti se tehničkim i organizacijskim mjerama zaštite što uključuje kontrolu korištenja razmjerno utvrđenim rizicima.

Članak 48.

Službena elektronička pošta mora se koristiti prvenstveno za službene svrhe odnosno obavljanje poslovnih zaduženja radnika te ne smije sadržavati materijal koji ima lažan, uznemiravajući, neugodan, seksualno eksplicitan, nepristojan, klevetnički ili bilo kakav drugi neprihvatljiv ili zakonski nedopušten sadržaj.

Korištenje interneta i elektroničke pošte detaljnije se uređuje uputama koje donosi ravnatelj Zavoda.

Korištenje kriptografskih kontrola

Članak 49.

Radi zaštite povjerljivosti i cjelovitosti osjetljivih informacija u informacijskom sustavu Zavoda koriste se kriptografske kontrole.

Kriptografske kontrole koriste se za zaštitu informacija pri:

- pohrani na poslužiteljima, korisničkim računalima, diskovnim sustavima te trakama i ostalim medijima
- prijenosu putem računalno-komunikacijskih mreža Zavoda
- radu s posebnim vrstama datoteka.

Fizička sigurnost osoba i imovine

Članak 50.

Mjere fizičke sigurnosti utvrđuju se radi smanjenja rizika i održavanja prikladne razine sigurnosti osoba u Zavodu (primjerice, osiguranih osoba, korisnika prava odnosno korisnika usluga Zavoda, radnika Zavoda, posjetitelja, vanjskih pružatelja usluga) i radi zaštite imovine.

Članak 51.

Zaštita osoba i imovine osigurava se primjenom odgovarajućih prostorno-tehničkih i organizacijskih mjera te primjenom mjera tjelesne i tehničke zaštite.

Fizički pristup svim poslovnim lokacijama Zavoda kontrolira se radi sprečavanja neovlaštenog ili nasilnog pristupa, krađe ili oštećenja informacijske imovine ili negativnih posljedica za zdravlje i sigurnost osoba.

Članak 52.

Poslovni prostori i objekti Zavoda kategoriziraju se u odnosu na pravo pristupa kao prostorije pod zaštitom i prostorije pod posebnom zaštitom.

Prostorije pod posebnom zaštitom u Zavodu trebaju biti jasno označene i dodatno zaštićene.

Mjere zaštite prostorija i objekata detaljnije se uređuju uputama koje donosi ravnatelj Zavoda.

Sigurnost operativnog postupanja s informacijskom imovinom

Članak 53.

Promjene na informacijskoj imovini Zavoda planiraju se ovisno o poslovnim i tehnološkim zahtjevima.

Zahtjev za promjenu može podnijeti vlasnik poslovnog procesa na koji se promjena odnosi ili voditelj projektnog tima, odnosno radne skupine.

Sve promjene na informacijskoj imovini moraju se testirati.

O promjenama na informacijskoj imovini obvezno se obavještavaju svi na koje se ta promjena odnosi.

Članak 54.

Upravljanje promjenama detaljnije se uređuje uputama koje donosi ravnatelj Zavoda.

Članak 55.

Korištenje informacijske imovine Zavoda obvezno se planira, nadzire i prilagođava prema unaprijed definiranim kriterijima i kontrolama.

Za sve aplikacije i usluge informatičkog sustava Zavoda utvrđuju se potrebni kapaciteti informatičke opreme radi postizanja zadanih funkcionalnosti i performansi aplikacija i usluga te sprječavanja zastoja u radu.

Članak 56.

U informatičkom sustavu Zavoda, ovisno o mogućnostima pojedinih dijelova sustava, elektronički se bilježe zapisi o stanju sustava, pristupanju i aktivnostima u sustavu.

Članak 57.

Vlasnik elektroničkog zapisa je vlasnik poslovnog procesa u okviru kojeg nastaje elektronički zapis i nadležan je za klasifikaciju elektroničkog zapisa, prava pristupa, korištenje, način čuvanja i arhiviranja, vrijeme čuvanja te način uništavanja elektroničkog zapisa.

Elektronički zapisi čuvaju se od gubitka, uništenja te neovlaštene izmjene, pristupa ili objave, u skladu sa zakonskim, podzakonskim, regulatornim, ugovornim i poslovnim zahtjevima.

Članak 58.

U Zavodu se radi povjerljivosti, cjelovitosti i raspoloživosti informatičke imovine, zaštite od zlonamjernog kôda te smanjenja ranjivosti sustava osigurava zasebno razvojno, testno i produkcijsko okruženje.

Članak 59.

Za sve poslovno važne dijelove informatičkog sustava (primjerice, baze podataka, aplikacije, datoteke vezane uz poslovne procese) Sektor za informatiku redovito izrađuje sigurnosne kopije kako bi se u slučaju kvara ili pada informatičkog sustava osigurao kontinuitet poslovanja i pružanja usluga Zavoda.

Članak 60.

Operativna postupanja na informacijskoj imovini obvezno se dokumentiraju i redovito nadziru.

Sigurnost računalnih komunikacija

Članak 61.

Radnicima Zavoda i vanjskim pružateljima usluga omogućava se pristup samo onim računalno- mrežnim podsustavima informatičkog sustava Zavoda za čiju su uporabu ovlašteni.

Računalno mrežni resursi i usluge moraju se koristiti tako da se ne ugrožava informacijska imovina ili umanjuje učinkovitost rada drugih korisnika sustava, usluga ili informatičke opreme.

Informacije uključene u prijenos putem internih i javnih mreža moraju biti zaštićene od neovlaštene izmjene ili otkrivanja, prijevara ili neovlaštene izmjene sadržaja.

Nabava, razvoj i održavanje sustava

Članak 62.

Poslove razvoja aplikacija i sistemskog održavanja informatičkog sustava Zavoda prvenstveno obavljaju radnici Zavoda.

Prema potrebi, obavljanje pojedinih ili svih aktivnosti u određenom procesu može se povjeriti vanjskim pružateljima usluga, u kojem slučaju Zavod obvezno nadzire i kontrolira obavljanje aktivnosti.

U metodologiji razvoja za sve razine arhitekture (poslovnu, aplikativnu i tehnološku) obvezno se vodi briga o sigurnosnim aspektima, u skladu s poslovnim mogućnostima.

Članak 63.

Pristup izvornom kôdu programa te izvođenje promjena na softverskim paketima dopušten je samo radnicima Sektora za informatiku Zavoda ili vanjskom pružatelju usluga, u skladu s ugovorom.

Tijekom testiranja nužno je pozorno birati informacije koje se koriste i izbjegavati korištenje stvarnih osobnih podataka, ako je to moguće.

Članak 64.

Pravila primjene sigurnosti unutar procesa nabave kao i sigurnosni zahtjevi u svim fazama nabave detaljnije se uređuju uputama koje donosi ravnatelj Zavoda.

Vanjski pružatelji usluga

Članak 65.

Vlasnik informacijske imovine i radnici zaduženi za pripremu ugovora s vanjskim pružateljima usluga dužni su prije sklapanja novih ugovora ili ažuriranja postojećih napraviti procjenu rizika i utvrditi kontrole za obradu odnosno upravljanje rizicima iz područja informacijske sigurnosti.

Ugovor s vanjskim pružateljem usluga i njegovim podizvođačima obvezno sadrži odredbe o kontrolama za upravljanje rizicima, odnosno uloge i odgovornosti za njihovu provedbu.

U ugovorima s vanjskim pružateljem usluga i njegovim podizvođačima treba specificirati sigurnosne zahtjeve za pristup i postupanje s povjerljivim informacijama, kao i obveze za prijavu incidenata informacijske sigurnosti.

Ugovori obvezno sadržavaju i odredbe koje omogućavaju nadzor nad izvršenjem i kontrolu mjera zaštite informacija odnosno informacijskog sustava koje provodi druga ugovorna strana.

Ugovori s vanjskim pružateljima usluga koji mogu utjecati na informacijsku sigurnost prije sklapanja obvezno se dostavljaju na suglasnost Uredu za poslovno-informacijsku sigurnost, kontrolu i nadzor.

Članak 66.

Prije sklapanja ugovora o poslovnoj suradnji, na temelju kojeg bi pravna ili fizička osoba imala pristup povjerljivim informacijama u Zavodu, obvezno se provodi provjera druge ugovorne strane. Provjera obuhvaća utvrđivanje je li pravna ili fizička osoba registrirana za obavljanje potrebne djelatnosti i osigurava li dovoljno jamstava da će poduzeti odgovarajuće mjere zaštite informacija.

Osoba odgovorna za praćenje izvršenja ugovora s vanjskim pružateljima usluga i rukovoditelj unutarnje ustrojstvene jedinice iz čijeg su djelokruga informacije odgovorni su za poduzimanje mjera za zaštitu informacija tijekom izvršavanja ugovora.

Članak 67.

Kada je za sklapanje ugovora o poslovnoj suradnji prethodno nužno omogućiti pristup informacijama, 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.

Pri suradnji s fizičkim i pravnim osobama, državnim i drugim tijelima i ustanovama u Republici Hrvatskoj, kao i s drugim državama i međunarodnim organizacijama, nužno je provesti procjenu mogućih rizika za informacijsku sigurnost Zavoda te poduzimati mjere zaštite za uklanjanje ili smanjivanje rizika.

Upravljanje incidentima informacijske sigurnosti

Članak 68.

Zavod održava i unaprjeđuje sustav upravljanja incidentima informacijske sigurnosti te osigurava učinkoviti odgovor, jasnu komunikaciju te pravodobnu identifikaciju i obradu ranjivosti.

Uloge i odgovornosti, procesi i alati relevantni za upravljanje incidentima informacijske sigurnosti detaljno se uređuju uputama koje donosi ravnatelj Zavoda.

Članak 69.

Svaki radnik Zavoda koji ima pristup informacijskoj imovini Zavoda dužan je, bez odgode, prijaviti incident i uočene ranjivosti informacijske sigurnosti, koristeći za to namijenjene komunikacijske kanale.

Svaka prijava incidenta i uočene ranjivosti informacijske sigurnosti obvezno se dokumentira, a saznanja prikupljena analizom i rješavanjem incidenata obrađuju se radi smanjenja vjerojatnosti ili negativnog učinka budućih incidenata.

Zaštita privatnosti radnika pri postupanju u slučaju incidenta

Članak 70.

U slučaju incidenta informacijske sigurnosti Zavod može nadzirati korištenje interneta i elektroničke pošte svakog pojedinačnog radnika Zavoda ako vrijednost dobra koje se želi zaštititi prevladava nad potrebom, odnosno pravom zaštite privatnosti radnika.

Pri analizi i obradi incidenata koriste se uvijek minimalno potrebne privatne informacije radnika.

O nadzoru iz stavka 1. ovog članka odlučuje ravnatelj Zavoda nakon savjetovanja sa službenikom za zaštitu podataka i savjetnikom za informacijsku sigurnost, uzimajući u obzir potrebe ažurnosti u prikupljanju informacija.

Upravljanje kontinuitetom poslovanja

Članak 71.

Zavod uspostavlja, održava i unaprjeđuje sustav pripreme i odgovora na izvanredne i krizne situacije, što uključuje analizu utjecaja na poslovanje, izradu i testiranje planova kontinuiteta poslovanja i planova oporavka od neželjenih situacija te stalnu edukaciju i osvještavanje radnika o načinima oporavka ključnih poslovnih procesa i aktivnosti.

Radi osiguranja kontinuiteta temeljnih i potpornih procesa Zavoda te kontrola informacijske sigurnosti, osiguravaju se potrebni pričuvni resursi u skladu s procjenom rizika i analizom utjecaja na poslovanje.

Članak 72.

Smatra se da je došlo do dugotrajnijeg zastoja u radu informatičkog sustava ako ključni dijelovi sustava, kao što su središnje računalo i računalno-komunikacijski sustav te poslužitelji Zavoda, nisu raspoloživi u vremenu duljem od identificiranog vremena oporavka, što može prouzročiti znatne poremećaje u radu Zavoda.

Članak 73.

U slučaju izvanrednih i kriznih situacija, postupa se prema planu i odlukama koje donosi ravnatelj Zavoda.

Plan postupanja u slučaju izvanrednih i kriznih situacija u radu informatičkog sustava Zavoda izrađuje se na osnovi analize utjecaja na poslovanje i obvezno sadrži:

- unaprijed pripremljene rezervne lokacije ili druge opcije na kojima će se moći odvijati poslovanje Zavoda
- prioritete poslovnih aktivnosti koje će se odvijati
- prioritete obrade informacija koje će se obavljati
- točan redoslijed i vrijeme ponovnog uspostavljanja poslovnih aktivnosti Zavoda.

Sukladnost i nadzor informacijske sigurnosti

Članak 74.

Savjetnik za informacijsku sigurnost vodi registar svih zakona, podzakonskih propisa, regulatornih i ugovornih zahtjeva relevantnih za informacijsku sigurnost, a o promjenama u registru obavještava poslovodstvo Zavoda.

U Zavodu se identificiraju, dokumentiraju i ažuriraju zahtjevi za zaštitu informacijskog sustava, prava intelektualnog vlasništva i softvera.

Članak 75.

Radnici Zavoda zaduženi za nadzor i internu procjenu (audit) informacijske sigurnosti planiraju, provode i dokumentiraju redovne i izvanredne interne procjene informacijske sigurnosti, u skladu sa zakonskim i podzakonskim propisima iz područja informacijske sigurnosti te općim aktima Zavoda.

Provedba redovitih i izvanrednih internih procjena detaljnije se uređuje uputama koje donosi ravnatelj Zavoda.

U Zavodu se redovito provode provjere tehničke sukladnosti.

Provjere tehničke sukladnosti obuhvaćaju, između ostalog, preglede operativnih sustava u smislu pravilne implementacije kontrola hardvera i softvera, penetracijska testiranja i provjere ranjivosti.

Članak 76.

Pomoćnik ravnatelja za informatiku donosi upute kojima se detaljnije uređuju sljedeća područja:

- konfiguracija i upravljanje prijenosnim računalima
- kontrola pristupa mreži i mrežnim servisima informacijskog sustava
- sigurnosni zahtjevi i upravljanje pristupom informacijskom sustavu
- pravila i savjeti za odabir i korištenje lozinki
- upotreba kriptografskih kontrola
- operativna postupanja (primjerice, pohranjivanje, testiranje odnosno ispitivanje valjanosti) sa sigurnosnim kopijama
- sigurnost računalnih komunikacija
- pravila primjene sigurnosti unutar procesa razvoja i održavanja kao i sigurnosni zahtjevi u svim fazama implementacije informatičkog sustava Zavoda, zajedno s kriterijima prihvaćanja i pravilima tehničke provjere nakon izvršenih promjena sustava/servisa.

VI. POVREDA OBVEZE ČUVANJA POVJERLJIVOSTI, CJELOVITOSTI I RASPOLOŽIVOSTI INFORMACIJA I MJERA ZAŠTITE INFORMACIJSKOG SUSTAVA

Članak 77.

Postupanjem protivno odredbama ovog Pravilnika, narušavanjem povjerljivosti, cjelovitosti i raspoloživosti informacijske imovine, odnosno nepoštivanjem utvrđenih mjera zaštite informacijskog sustava, radnik Zavoda čini osobito tešku povredu obveze iz radnog odnosa i odgovara prema odredbama Zakona o radu za eventualnu štetu prouzročenu poslodavcu.

Prema članu Upravnog vijeća ili drugoj osobi koja nije radnik Zavoda, a koja naruši povjerljivost, cjelovitost ili raspoloživost informacijske imovine ili informacijskog sustava, poduzet će se odgovarajuće mjere, u skladu s propisima odnosno ugovorom i zahtijevat će se nadoknada eventualno nanesene štete Zavodu.

Povredom obveze čuvanja povjerljivosti ne smatra se priopćenje koje osoba upoznata s povjerljivim informacijama iznese u prijavi kaznenog djela ili u drugom slučaju kada za to postoji zakonska obveza.

VII. ZAVRŠNE ODREDBE

Članak 78.

U roku od šest mjeseci od dana stupanja na snagu ovog Pravilnika donijet će se:

- Plan postupanja u slučaju izvanrednih ili kriznih situacija iz članka 73. ovog Pravilnika
- Upute za rad iz članka 76. ovog Pravilnika.

Članak 79.

Na dan stupanja na snagu ovog Pravilnika prestaje važiti Pravilnik o zaštiti informacijskog sustava i tajnosti podataka u Hrvatskom zavodu za mirovinsko osiguranje, KLASA: 041-01-14-02/11, URBROJ: 341-99-01/01-14-8, od 18. prosinca 2014.

Članak 80.

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

KLASA: 140-01/21-07/1
URBROJ: 341-99-01/7-21-1
Zagreb, 26. srpnja 2021.

RAVNATELJ
Ivan Serdar

OBRAZLOŽENJE

Zakonom o informacijskoj sigurnosti (NN 79/07), Uredbom o mjerama informacijske sigurnosti (NN 46/08) te ostalim provedbenim aktima cjelovito se uređuje sustav informacijske sigurnosti tako da se propisuju mjere i standardi koje su tijela javne vlasti obvezna provoditi radi zaštite povjerljivosti, cjelovitosti i raspoloživosti informacija koje se u poslovnim informacijskim sustavima stvaraju, prikupljaju, obrađuju, prenose i razmjenjuju.

U Zavodu se primjenjuje Pravilnik o zaštiti informacijskog sustava i tajnosti podataka u Hrvatskom zavodu za mirovinsko osiguranje koji je donesen 18. prosinca 2014.

Od donošenja navedenog Pravilnika, sustav informacijske sigurnosti u Zavodu kontinuirano se unaprjeđuje te je Zavod tijekom 2018. i 2019. godine implementirao sustav upravljanja informacijskom sigurnošću u skladu sa zahtjevima međunarodne norme ISO/IEC 27001:2013 i zbog toga se donosi novi pravilnik.

Prijedlog novog pravilnika o informacijskoj sigurnosti usklađen je sa zahtjevima međunarodne norme ISO/IEC 27001:2013, a pri izradi prijedloga uzete su u obzir i preporuke Ureda za reviziju u vezi s usklađivanjem internih akata informacijske sigurnosti radi smanjenja rizika neujednačenog postupanja u praksi.

Pravilnikom nije moguće obuhvatiti sve mjere zaštite, postupke i standarde koji se odnose na informacijsku sigurnost u Zavodu, stoga je dio specifičnih kontrola propisan i drugim općim aktima (primjerice, općim aktima o upravljanju projektima, zaštiti od požara, o radu, zaštiti na radu, o pravu na pristup informacijama, o upravljanju dokumentarnim gradivom).
Kako Zavod u svom radu raspolaže pretežno osobnim podacima, dodatne mjere zaštite osobnih podataka utvrdit će se zasebnim općim aktom.

Za zaštitu tajnih ili klasificiranih informacija zaprimljenih od drugih tijela, uz mjere utvrđene novim Prijedlogom pravilnika, primjenjuju se dodatno i druge mjere i standardi u skladu sa zakonskim i podzakonskim propisima iz područja informacijske sigurnosti i tajnosti podataka.

Radi učinkovite provedbe mjera za obradu rizika informacijske sigurnosti, za potrebe pojedinih poslovnih procesa u unutarnjim ustrojstvenim jedinicama Zavoda donijet će se upute za rad koje se temelje na kontrolama sadržanima u Aneksu A međunarodne norme ISO/IEC 27001:2013.