Hrvatski zavod za mirovinsko osiguranje

STRATEGIJA INFORMACIJSKE SIGURNOSTI U HRVATSKOM ZAVODU ZA MIROVINSKO OSIGURANJE 2014. – 2017.

Zagreb, 13. travnja 2014.

V1.3 nakon primjedbi Sektora

Sadržaj

Str.

I. Uvod 2

II. Normativni okvir 3

III. Postojeće stanje 5

Pravni akti Zavoda 5

Projekt „Uvođenje sustava za upravljanje informacijskom sigurnošću u Zavodu“ 7

Zaključak o stanju informacijske sigurnosti u HZMO-u 9

IV. Utvrđivanje vizije i strateških ciljeva 10

V. Određivanje mjera i prioriteta 11

I. Uvod

Pojam informacijske sigurnost u ovom dokumentu obrađuje se na način kakav je danas prihvaćen u razvijenim zemljama svijeta i koji osigurava sukladnost s konceptom informacijske sigurnosti NATO-a i EU. Sustav informacijske sigurnosti, sukladno Zakonu o tajnosti podataka i Zakonu o informacijskoj sigurnosti, obuhvaća ljude, procese, organizaciju i tehnologiju. Taj se sustav sastoji od uravnoteženog skupa sigurnosnih mjera: sigurnosne provjere osoblja, fizičke sigurnosti, sigurnosti podataka, sigurnosti informacijskih sustava; te koordiniranog uvođenja formalnih procedura poput procjene rizika, certifikacije osoblja i uređaja, kao i akreditacije tehničkih sustava za primjenu u određenom segmentu poslovnog procesa državne uprave. Uravnoteženost i koordinacija bitnih mjera i postupaka postižu se organizacijom i upravljanjem informacijskom sigurnošću.

Informacijska sigurnost bavi se zaštitom informacija koje Zavod prikuplja, čuva, obrađuje i isporučuje bez obzira na to u kojem se obliku informacije nalaze (elektroničkom ili papirnatom). Informacije treba zaštititi od uništenja, neovlaštenog pristupa i neovlaštene izmjene. Većina mogućih opasnosti za informacije dolazi od zainteresiranih osoba, a informacije treba zaštititi i od više sile (poplava, potres, požar…).

Zakon o informacijskoj sigurnosti propisuje obvezu provedbe informacijske sigurnosti za sva tijela državne uprave, jedinice lokalne i područne samouprave, pravne osobe s javnim ovlastima koje ostvaruju pristup klasificiranim i neklasificiranim podatcima. Zakon o zaštiti osobnih podataka propisuje tu obvezu za navedena tijela koja prikupljaju osobne podatke u skladu sa Zakonom o zaštiti osobnih podataka.

Sustav informacijske sigurnosti razrađuje se, promatrajući sve mjere, standarde i nadležnosti tijela, podjelom na pet međunarodno prihvaćenih sigurnosnih područja informacijske sigurnosti u državnim upravama: sigurnosne provjere, fizička sigurnost, sigurnost podataka, sigurnost informacijskih sustava i sigurnost vanjske suradnje.

Budući da Zavod u svom poslovanju stvara, prikuplja, obrađuje i prenosi velik broj podataka koji se odnose na osiguranike, korisnike i radnike Zavoda, potrebno je, radi osiguranja povjerljivosti, cjelovitosti i raspoloživosti podataka, osigurati sve mjere informacijske sigurnosti koje će onemogućiti moguće ugroze sustava informacijske sigurnosti.

Cilj je ove strategije postaviti cjelovit plan razvoja informacijske sigurnosti Hrvatskog zavoda za mirovinsko osiguranje, kojim će se odrediti glavne aktivnosti za izgradnju i provedbu sustava informacijske sigurnosti u sljedećem srednjoročnom razdoblju (3 – 5 godina).

II. Normativni okvir

Zakonom o informacijskoj sigurnosti, a potom i Uredbom o mjerama informacijske sigurnosti te ostalim provedbenim aktima prvi put se cjelovito uređuje sustav informacijske sigurnosti na način da se propisuje cijeli niz mjera i standarda koje tijela javne vlasti moraju provesti radi ostvarivanja stanja povjerljivosti, cjelovitosti i raspoloživosti podataka. Mjere informacijske sigurnosti predstavljaju opća pravila zaštite podataka koji se realiziraju na fizičkoj, tehničkoj ili organizacijskoj razini.

Propisi koji uređuju područje informacijske sigurnosti su:

1. Nacionalni program informacijske sigurnosti u RH

   Programom koji je donesen u ožujku 2005. utvrđuju se ciljevi informacijske sigurnosti na razini Republike Hrvatske, nadležnosti i poslovi pojedinih institucija u području informacijske sigurnosti, kao i potrebna međusobna koordinacija svih čimbenika informacijske sigurnosti.

2. Zakon o zaštiti osobnih podataka (Narodne novine, broj 103/2003, 118/2006, 41/2008, 130/2011 i 106/2012- pročišćeni tekst)

   Zakonom se uređuje zaštita osobnih podataka o fizičkim osobama te nadzor nad prikupljanjem, obradom i korištenjem osobnih podataka u Republici Hrvatskoj.

3. Zakon o informacijskoj sigurnosti (Narodne novine, broj 79/2007- u daljnjem tekstu Zakon)

   Zakonom se utvrđuje pojam informacijske sigurnosti, mjere i standardi informacijske sigurnosti, područja informacijske sigurnosti te nadležna tijela za donošenje, provedbu i nadzor mjera i standarda informacijske sigurnosti

4. Zakon o tajnosti podataka (Narodne novine, broj 79/2007 i 86/2012)

   Zakonom se utvrđuje pojam klasificiranih i neklasificiranih podataka, stupnjevi tajnosti, postupak klasifikacije i deklasifikacije, pristup klasificiranim i neklasificiranim podatcima, njihova zaštita i nadzor nad provedbom ovoga Zakona.

5. Zakon o sigurnosnoj provjeri (Narodne novine, broj 85/2008)

   Zakonom se utvrđuje pojam, vrste i stupnjevi sigurnosne provjere, sigurnosne zapreke te postupak njihove provedbe.

6. Uredba o mjerama informacijske sigurnosti (Narodne novine, broj 46/2008)

   Uredbom se utvrđuju mjere informacijske sigurnosti za postupanje s klasificiranim i neklasificiranim podatcima.

7. Uredba o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka (Narodne novine, broj 139/2004)

   Uredbom se određuju mjere, sredstva i uvjeti pohranjivanja, osiguranja i zaštite te prijenosa posebnih kategorija osobnih podataka i zbirki takvih podataka, mjere održavanja i provjere ispravnosti rada računalne, telekomunikacijske i programske opreme sustava za vođenje zbirki posebnih kategorija osobnih podataka, osiguranje radnih prostorija u kojima je smještena ta oprema, osobe ovlaštene za provedbu planiranih mjera te osobe odgovorne za nadzor nad provedbom tih mjera.

8. Uredba o načinu označavanja klasificiranih podataka, sadržaju i izgledu uvjerenja o obavljenoj sigurnosnoj provjeri i izjave o postupanju s klasificiranim podacima (Narodne novine, broj 102/2007)

   Uredbom se propisuje način označavanja klasificiranih i neklasificiranih podataka, sadržaj i izgled uvjerenja o obavljenoj sigurnosnoj provjeri te sadržaj i izgled izjave o postupanju s klasificiranim podatcima.

9. Pravilnik o kriterijima za ustrojavanje radnih mjesta savjetnika za informacijsku sigurnost (Narodne novine, broj 100/2008)

   Pravilnikom se utvrđuju kriteriji za ustrojavanje radnih mjesta i imenovanje savjetnika za informacijsku sigurnost.

10. Uredba o načinu vođenja i obrascu evidencije o zbirkama osobnih podataka (Narodne novine, broj 105/2004)

    Uredbom se propisuje način vođenja evidencije o zbirkama osobnih podataka koje vode državna tijela, tijela lokalne i područne (regionalne) samouprave te fizičke i pravne osobe koje obrađuju osobne podatke (u daljnjem tekstu: voditelji zbirke osobnih podataka) i propisuje se obrazac te evidencije.

11. Uredba o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka (Narodne novine, broj 139/2004)

    Uredbom se određuju mjere, sredstva i uvjeti pohranjivanja, osiguranja i zaštite te prijenosa posebnih kategorija osobnih podataka i zbirki takvih podataka, mjere održavanja i provjere ispravnosti rada računalne, telekomunikacijske i programske opreme sustava za vođenje zbirki posebnih kategorija osobnih podataka (u daljnjem tekstu: sustav), osiguranje radnih prostorija u kojima je smještena ta oprema, osobe ovlaštene za provedbu planiranih mjera te osobe odgovorne za nadzor nad provedbom tih mjera.

12. Pravilnik o standardima sigurnosne provjere (UVNS, neklasificirano)
13. Pravilnik o standardima fizičke sigurnosti (UVNS, neklasificirano)
14. Pravilnik o standardima sigurnosti podataka (UVNS, neklasificirano)
15. Pravilnik o standardima organizacije i upravljanja područjem sigurnosti informacijskih sustava (UVNS, neklasificirano)
16. Pravilnik o standardima sigurnosti poslovne suradnje (UVNS, neklasificirano)
17. Pravilnik o standardima sigurnosti informacijskih sustava (ZSIS, neklasificirano)
18. Pravilnik o prevenciji i odgovoru na računalno-sigurnosne ugroze (ZSIS, neklasificirano)
19. Pravilnik o sigurnosnoj akreditaciji (ZSIS, neklasificirano).

Zakon o informacijskoj sigurnosti kojim je prvi put cjelovito uređen sustav informacijske sigurnosti u RH kao dio sustava nacionalne sigurnosti, ali i suvremenog informacijskog sustava, primjenjuje se na državna tijela, tijela jedinice lokalne i područne samouprave te pravne osobe s javnim ovlastima koje u svom djelokrugu koriste klasificirane i neklasificirane podatke.

III. Postojeće stanje

Pravni akti Zavoda

Budući da se u najvećem dijelu radi o osobnim podatcima, Zavod je u skladu s odredbama Zakona o zaštiti osobnih podataka proveo sve mjere vezane uz obradu osobnih podataka. U skladu s člankom 18a. Zakona Zavod je imenovao službenika za zaštitu osobnih podataka. Pri postupanju s osobnim podatcima, Zavod strogo poštuje odredbe Zakona o zaštiti osobnih podataka, a u slučajevima koji zahtijevaju dodatna pojašnjenja službenik za zaštitu osobnih podatka dodatno se konzultira s Agencijom za zaštitu osobnih podataka.

Zavod je također donio određene opće akte i upute kojima su u poslovanje Zavoda uvedeni određeni sigurnosni čimbenici, uvažavajući činjenicu da postoji cijeli niz segmenata u informacijskom i infrastrukturnom području poslovanja koji zahtijevaju uvođenje odredbi i procedura u postupanju radi zaštite cjelokupnog informacijskog sustava. Prepoznato je da informacijski sustav ne uključuje samo IT tehnologiju, već i rješavanje određenih organizacijskih preduvjeta, upravljanje ljudskim resursima. Dakle, informacijska sigurnost premašuje dosege Sektora za informatiku. Navedeno se vidi iz popisa akata i uputa koje je Zavod donio u prethodnom razdoblju i čijim se donošenjem nastojao uspostaviti sustav informacijske sigurnosti.

S obzirom na to da je svijest o potrebi čuvanja informacija u Zavodu bila na visokoj razini i prije prethodno navedene regulative, u Zavodu postoje akti koji djelomično uređuju informacijsku sigurnost:

1. Pravilnik o pravu na pristup informacijama

   Pravilnikom se u skladu sa Zakonom o pravu na pristup informacijama, a radi ostvarivanja javnosti rada HZMO-a, utvrđuju načini ostvarivanja prava i iznimke u vezi s ostvarivanjem prava na pristup informacijama Zavoda te organizacija postupanja i rješavanja o zahtjevima unutar Zavoda. Pravilnik je stupio na snagu 27. srpnja2011.

2. Pravilnik o zaštiti informatičke opreme, mreže, dokumentacije i podataka

   Pravilnikom se utvrđuju načini i mjere zaštite informatičke opreme, mreže, dokumentacije i podataka koji se prikupljaju, bilježe i obrađuju primjenom informatičke opreme u HZMO-u. Pravilnik je stupio na snagu 26. svibnja2004.

3. Pravilnik o arhivskom i registraturnom gradivu

   Pravilnikom se uređuje zaštita, uvjeti odlaganja i čuvanja arhivskoga gradiva, postupak odabiranja i izlučivanja registraturnoga gradiva te način uništenja izlučenoga gradiva u Hrvatskom zavodu za mirovinsko osiguranje, kao i pitanja predaje arhivskoga gradiva nadležnom arhivu. Pravilnik je stupio na snagu 27. ožujka2004.

4. Pravilnik o zaštiti tajnosti podataka i priopćavanja javnosti informacija o radu HZMO-a

   Pravilnikom se uređuje koji se podatci u HZMO-u smatraju poslovnom i profesionalnom tajnom, stupnjevi tajnosti, mjere i postupci za utvrđivanje, čuvanje, priopćavanje i uporabu tih podataka te priopćavanje javnosti informacija o poslovanju Zavoda, radu njegovih tijela i njegove stručne službe. Pravilnik je donesen 25. ožujka2002.

5. Pravilnik o zaštiti od požara

   Pravilnikom se uređuje sustav zaštite od požara u HZMO-u u skladu sa Zakonom o zaštiti od požara, propisima donesenim na temelju zakona te planovima i potrebama Zavoda. Pravilnik je donesen 30. travnja2013.

6. Pravilnik o upravljanju projektima u HZMO-u

   Pravilnikom se uređuje organizacija, metode projektiranja i provedba projekata, sudionici i njihovi zadatci u radu na projektima, međusobna komunikacija sudionika na projektima, izvještavanje o projektima, projektna dokumentacija te druga pitanja u vezi s projektiranjem u Hrvatskom zavodu za mirovinsko osiguranje. Pravilnik je stupio na snagu 10. studenoga2010.

7. Pravilnik o radu

   Pravilnikom se uređuje zasnivanje radnog odnosa, radno vrijeme i raspored radnog vremena, trajanje godišnjeg odmora i dopusta, plaća, naknada plaće i materijalna prava i obveze radnika Zavoda i druga pitanja u vezi s radom.

8. Upute za rukovanje informatičkom i mikrografskom opremom

   Uputom su utvrđene potrebe Zavoda za praćenje smještaja i kretanja informatičke i mikrografske imovine (od trenutka zaprimanja do otpisa). Uputa je donesena u ožujku 2011.

9. Upute Prijava korisnika u IMS

   Neformalna uputa kojom se određuje način izmjene lozinke pri prijavljivanju u IMS.

10. Upute za korisnike MS Outlooka

    Uputa je namijenjena informatičarima PS/PU i SS te ostalim radnicima HZMO-a radi namještanja i korištenja MS Exchange sustava elektroničke pošte. Uputa je donesena u studenome 2013.

11. Upute za prijavu i odjavu s mreže

    Uputom su utvrđeni osnovni postupci za korisnike računala u radu mrežnog okruženja i obuhvaćaju postupke prijave i odjave korisnika s mreže te kreiranje i izmjenu mrežne lozinke. Uputa je donesena u studenome 2008.

12. Upute za rad s aplikacijom Servisnog centra

    Uputom su obuhvaćeni osnovni postupci radnika HZMO-a u radu s aplikacijom Servisnog centra. Uputa je donesena u listopadu 2011.

13. Uputa o prijavi na TSO te radu s aplikacijom za administriranje identifikacijskim podacima korisnika središnjih baza podataka HZMO-a

    Upute su namijenjene zaposlenima u područnim službama koji su zaduženi za obavljanje poslova iz informatičke djelatnosti kojima se dio administracije s korisničkim imenima i lozinkama za rad sa središnjim bazama podataka prenosi iz SI na informatičare u područnim službama. Uputa je donesena u ožujku 2005.

14. Uputa o generiranju, promjeni i pohrani zapisa lozinke koja omogućava najviša prava pristupa pojedinačnom računalu u informatičkom sustavu HZMO-a

    Uputom se utvrđuje rad i odgovornost radnika na poslovima administratora pojedinačnih računala informatičke mreže HZMO-a u dijelu generiranja, promjene i

pohrane lozinke s najvišim pravom pristupa pojedinačnom računalu. Uputa je donesena u ožujku 2005.

15. Upute o organizaciji mikrografske obrade dokumenata

    Uputama se uređuje predmet i oblik snimanja te područna organizacija mikrografske obrade, priprema dokumentacije za mikrografsku obradu, primopredaja dokumentacije i mikrografskih nositelja podataka, mikrografska obrada dokumentacije te nadležnosti zaštite i čuvanja dokumentacije, korištenje mikrografskih nositelja podataka, čuvanje i zaštita mikrografskih nositelja podataka te primjena uputa. Uputa je donesena 2004.

16. Upute za korištenje interneta i elektroničke pošte u HZMO-u

    Uputama se utvrđuju pravila za korištenje interneta i elektroničke pošte u HZMO-u po kojima mora postupati svaki radnik Zavoda pri korištenju interneta i elektroničke pošte.

    Uputa je donesena u studenome 2003.

17. Call centar- upute za rad

    Uputama se utvrđuju postupci primanja telefonskih poziva, tj. upita građana, davanje odgovora, informacija, odnosno pružanje pomoći strankama. Uputa je donesena u siječnju 2003.

18. Upute za ažuriranje internetske stranice HZMO-a

    Uputa je donesena u kolovozu 2004.

Upute i akti Zavoda razvijani su prema trenutačnim potrebama, ali su dobar temelj za čuvanje sigurnosti informacija u Zavodu. U ovom trogodišnjem razdoblju potaknut će se revizija navedenih internih akata Zavoda.

Projekt „Uvođenje sustava za upravljanje informacijskom sigurnošću u Zavodu“

U svibnju 2011. u Zavodu je započeo rad na projektu „Uvođenje sustava za upravljanje informacijskom sigurnošću u Zavodu“.

U suradnji s vanjskim konzultantom, stručnjaci Zavoda su u skladu s metodologijom rada na uvođenju standarda ISO 27001 izradili snimku stanja koja je ujedno i procjena rizika kao početni korak u uvođenju sustava informacijske sigurnosti.
U prvoj fazi uvođenja sustava za upravljanje informacijskom sigurnošću napravljena je prva procjena informacijskih rizika u Zavodu i pripremljeni su dokumenti kao što su politike, procedure i upute koji sadrže kriterije za potpuni nadzor informacijske sigurnosti u Zavodu.
Dokumenti su uređeni prema metodologiji standarda HRN ISO/IEC 27001 na koju nas obvezuje Uredba o mjerama informacijske sigurnosti (NN br. 46/08).
Ukupno je napravljeno 25 dokumenata koji će uz postojeće akte Zavoda osigurati informacijsku sigurnost Zavoda primjerene razine.

Krovni dokumenti:

- Odluka o opsegu sustava za upravljanje informacijskom sigurnošću
- Politika sustava za upravljanje informacijskom sigurnošću
- Procedura za upravljanje dokumentacijom i zapisima

- Pravilnik o zaštiti informatičkog sustava, dokumentacije i podataka

Dokumenti namijenjeni svim sudionicima sustava:

- Politika pravilne uporabe informacijskih resursa
- Politika rukovanja klasificiranim informacijama
- Uputa za rukovanje klasificiranim informacijama

Procjena rizika informacijske sigurnosti i djelovanje na njih:

- Metodika za procjenu i obradu rizika
- Procjena rizika
- Obrada rizika
- Izvještaj o procjeni rizika
- Izvještaj o primjenjivosti

Dokumenti za kontrolu pristupa informacijama:

- Politika kontrole pristupa
- Politika uklanjanja i uništavanja
- Uputa za nadzor uporabe informacijskog sustava
- Izjava o povjerljivosti

Razvoj i održavanje sustava:

- Procedura upravljanja promjenama
- Uputa za specificiranje sigurnosnih zahtjeva
- Politika sigurnosnih kopija

Dokumenti koji uređuju odnose s vanjskim partnerima:

- Politika razmjene informacija
- Uputa za uređivanje sigurnosnih pitanja s dobavljačima i partnerima

Upravljanje incidentima:

- Procedura za upravljanje incidentima
- Procedura za korektivne i preventivne mjere

Kontrola sustava:

- Procedura za interni audit

Osvješćivanje i naobrazba:

- Politika osvješćivanja i izobrazbe

Zaključak o stanju informacijske sigurnosti u HZMO-u

Zaključak je Radne skupine koja je radila snimku stanja informacijske sigurnosti da je sustav informacijske sigurnosti u Zavodu zadovoljavajući. Zavod je donio niz akata i procedura za postupanj u svrhu reguliranja područja informacijske sigurnosti, no budući da su zakonski propisi kojima se uređuje ovo područje prvi put cjelovito utvrdili okvir za postupanje i uspostavljanje informacijske sigurnosti, Zavod kao pravna osoba s javnim ovlastima mora uskladiti svoj sustav informacijske sigurnosti u skladu sa zakonskim propisima radi povećanja sigurnosti poslovanja u uvjetima sve veće ovisnosti o informacijskim tehnologijama.

Vezano uz imenovanje savjetnika za informacijsku sigurnost, u skladu sa Zakonom o informacijskoj sigurnosti i Pravilnikom o kriterijima za ustrojavanje radnih mjesta savjetnika za informacijsku sigurnost, može se zaključiti da tijela koja u svom radu koriste neklasificirane podatke ne moraju ustrojiti radno mjesto savjetnika za informacijsku sigurnost, no s obzirom na važnost informacijske sigurnosti u današnjem poslovanju, potrebno je odrediti radnika u svakom tijelu javne vlasti koji će nadzirati postupke organizacije, provedbe i učinkovitosti mjera i standarda informacijske sigurnosti te bi i Zavod trebao odrediti jednu osobu koja bi obavljala navedene poslove.

Napomena: Za detaljnije informacije o stanju informacijske sigurnosti u Zavodu treba pogledati dokument „Snimka stanja informacijske sigurnosti u Zavodu“ (siječanj 2014.)

IV. Utvrđivanje vizije i strateških ciljeva

Vizija informacijske sigurnosti u Zavodu koja se može definirati kao „uspostava sustava za upravljanje informacijskom sigurnošću sa što potpunijom zaštitom informacija u vlasništvu HZMO, uz poštivanje međunarodnih standarda za upravljanje informacijskom sigurnošću“ mora biti polazna točka u određivanju strateškog cilja uspostave sustava.

Strateški cilj Zavoda na području informacijske sigurnosti je uvođenje takvog sustava za upravljanje informacijskom sigurnošću, tj. uvođenje pisanih postupaka (procedura), koji će osigurati:

- dostupnost, povjerljivost i cjelovitost informacija koje nastaju i koriste se u poslovnim procesima Zavoda, u skladu s važećim zakonskim aktima iz područja informacijske sigurnosti
- stalni nadzor nad funkcioniranjem sustava za upravljanje informacijskom sigurnošću Zavoda i kontrolu djelotvornosti sustava od strane rukovodstva Zavoda
- stalno unaprjeđivanje i poboljšavanje sustava za upravljanje informacijskom sigurnošću
- usklađenost pravne regulative Zavoda s važećim zakonskim propisima.

Svrha uspostavljanja sustava za upravljanje informacijskom sigurnošću je što potpunija zaštita informacija kojima Zavod raspolaže, bez obzira na to u kojem se obliku nalaze. Uspostavljanje sustava za upravljanje informacijskom sigurnošću je zahtjevan proces u kojem moraju sudjelovati svi radnici Zavoda koji mogu utjecati na povjerljivost, cjelovitost i dostupnost informacija, a čelnici Zavoda trebaju pružiti punu podršku uvođenju i djelovanju sustava.Osim toga, uvođenje sustava za upravljanje informacijskom sigurnošću je i obveza svih javnih i državnih ustanova u Republici Hrvatskoj.

V. Određivanje mjera i prioriteta

Radi realizacije postavljenih ciljeva, potrebno je provesti sljedeće mjere:

1. Uskladiti akte Zavoda sa zakonskim propisima iz područja informacijske sigurnosti

   Pravni okvir kojim je do sada djelomično uređeno područje informacijske sigurnosti u Zavodu prema navedenom popisu akata potrebno je uskladiti neovisno o propisima koji su doneseni od 2007., a odnose se na Zakon o informacijskoj sigurnosti i provedbene propise u vezi s informacijskom sigurnosti. Određeni opći akti i upute donesene su početkom 2000. pa bi ih s obzirom na takav vremenski odmak trebalo ažurirati i prilagoditi postojećem okruženju i novim tehnologijama koje su uvedene, odnosno koje se uvode u poslovanje Zavoda.

   Planirane aktivnosti:
   - Pratiti izmjene u zakonskoj regulativi i usklađivati akte Zavoda s promjenama

2. Nastaviti rad na projektu „Uvođenje sustava za upravljanje informacijskom sigurnošću u Zavodu“

   Norma HRN ISO/IEC 27001 je međunarodni standard za upravljanje informacijskom sigurnošću i podloga je za izradu politika, procedura i uputa u okviru navedenog projekta. Aneks A norme sadrži ukupno 11 poglavlja unutar kojih se nalaze ukupno 133 mjere (kontrole) koje predstavljaju katalog sigurnosnih mjera koje se koriste tijekom postupka obrade rizika.
   Poglavlja Aneksa A:
   1) Sigurnosna politika
   2) Organizacija informacijske sigurnosti
   3) Upravljanje resursima
   4) Sigurnost vezana uz osoblje
   5) Fizička sigurnost i sigurnost okruženja
   6) Upravljanje komunikacijama i operativnim postupcima
   7) Kontrola pristupa
   8) Nabava, razvoj i održavanje informacijskih sustava
   9) Upravljanje incidentima informacijske sigurnosti
   10) Upravljanje kontinuitetom poslovanja
   11) Sukladnost.

   Implementacijom projekta, tj. donošenjem pisanih postupaka dobiva se jasno utvrđen okvir nadležnosti, odgovornosti i ovlasti unutar informacijskog sustava Zavoda. Usvajanjem procedura u okviru projekta detaljno se određuje odgovornost, zaštita i klasifikacija podataka, područje sustava, uporaba interneta i intraneta te suradnja s korisnicima izvan sustava.

Na temelju procjene rizika koja predstavlja snimku stanja informacijske sigurnosti započinje rad na analizi informacijske sigurnosti. Kada se u postupku procjene rizika utvrde neprihvatljivi rizici, aneks A pomaže u odabiru kontrola kojima će se omogućiti smanjivanje rizika.

Nakon završetka postupka obrade rizika utvrđuju se mjere iz Aneksa A koje su potrebne za uspostavljanje sustava informacijske sigurnosti. Propisano je da se za ostvarenje pojedinih mjera propišu procedure odvijanja procesa odgovarajućim aktima.

Planirane aktivnosti na projektu:

- raspraviti o pripremljenim dokumentima te ih po potrebi izmijeniti i dopuniti
- usvojiti dokumentaciju
- primijeniti usvojenu dokumentaciju.

3. Kontinuirano pratiti funkcioniranje sustava za upravljanje sigurnošću nakon njegove uspostave u Zavodu.

Nakon uvođenja sustava u primjenu potrebno je uspostaviti stalni nadzor radi procjene funkcioniranja sustava i eventualnog poboljšanja.

Planirane aktivnosti na nadzoru sustava:

- imenovati osobu koja će obavljati poslove koordinatora za informacijsku sigurnost
- kontinuirano pregledavati i dopunjavati cjelokupnu dokumentaciju koja uređuje informacijsku sigurnost u Zavodu.

4. Izraditi plan aktivnosti za provedbu mjera utvrđenih ovom strategijom.

Nakon usvajanja strategije potrebno je izraditi detaljan plan aktivnosti za svaku planiranu mjeru koji će sadržavati predviđene aktivnosti, njihove nositelje, rokove završetka i rezultate (isporuke).

Ovaj plan aktivnosti bit će donesen u roku 60 dana od usvajanja ovog dokumenta.