Agencija za lijekove i medicinske proizvode

Na temelju članka 21 Statuta Agencije za lijekove i medicinske proizvode, a u vezi s člankom 24. stavkom 1. Zakona o informacijskoj sigurnosti (Narodne novine, br. 79/07, 14/24), Upravno vijeće Agencije za lijekove i medicinske proizvode donosi

Pravilnik o provedbi mjera i standarda informacijske sigurnosti

Agencije za lijekove i medicinske proizvode

1. OPĆE ODREDBE

Članak 1.

Pravilnikom o informacijskoj sigurnosti u Agenciji za lijekove i medicinske proizvode (u daljnjem tekstu: Pravilnik) utvrđuju se:

- uloge i odgovornosti u sustavu upravljanja informacijskom sigurnošću,
- mjere i standardi informacijske sigurnosti,
- zahtjevi u području povjerljivosti, cjelovitosti i raspoloživosti informacijske imovine.

Ovim Pravilnikom utvrđen je skup mjera informacijske sigurnosti sukladno normi za upravljanje informacijskom sigurnošću IS0/IEC 27001:2022.

Članak 2.

Agencija za lijekove i medicinske proizvode (u daljnjem tekstu: Agencija) u obavljanju poslova iz svoje nadležnosti postupa s neklasificiranim podacima.

Podatak koji je označen oznakom „Neklasificirano“ koristi se isključivo u službene svrhe i može biti dostupan onim fizičkim i pravnim osobama koje imaju potrebu korištenja takvog podatka u službene svrhe i radi obavljanja poslova iz njihova djelokruga.

Postupanje s klasificiranim podacima označenim određenim stupnjevima tajnosti propisat će se standardnim operativnim postupkom.

Članak 3.

Ovaj Pravilnik primjenjuje se na sve zaposlenike i procese Agencije, vanjske suradnike, članove povjerenstava i Upravnog vijeća Agencije pri rukovanju informacijskom imovinom Agencije, a radi zaštite povjerljivosti, cjelovitosti i dostupnost podataka i informacija.

Članak 4.

Na upravljanje informacijskom sigurnošću primjenjuju se načela i mjere propisane ovim Pravilnikom, Politikom kibernetičke sigurnosti, Poslovnikom kakvoće Agencije, standardnim operativnim postupcima i međunarodnom normom IS0/IEC 27001:2022.

Članak 5.

Pojedini pojmovi u smislu ovog Pravilnika imaju sljedeće značenje:

1) Cjelovitost je svojstvo informacije koje se odnosi na izvornost i potpunost, uz sprječavanje neovlaštene izmjene sadržaja,
2) Incident informacijske sigurnosti je neželjeni ili neočekivani događaj koji narušava povjerljivost, cjelovitost ili raspoloživost informacijske imovine, odnosno događaj (realizacija prijetnje zbog ranjivosti) koji ima značajnu vjerojatnost ugroze poslovnih aktivnosti (kao npr. nepravilnost u radu sustava ili preopterećenje sustava, ljudska pogreška, gubitak opreme ili uređaja, odavanje povjerljivih informacija, itd..),
3) Informacija je jedan ili više podataka s pripisanim značenjem,
4) 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: dokumentacija, baze podataka, procesi, aplikacije, informatička oprema, uredski prostori),
5) Informacijska sigurnost je stanje povjerljivosti, cjelovitosti i raspoloživosti podataka koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda,
6) Informacijski sustav (informatički sustav) je komunikacijski, računalni ili drugi elektronički sustav u kojem se podaci obrađuju, pohranjuju ili prenose, tako da budu dostupni i upotrebljivi za ovlaštene korisnike,
7) Korisnik informacijskog sustava je svaka osoba koja koristi Agencijski informacijski sustav (zaposlenici Agencije, vanjski suradnici, vanjski pružatelji usluga, i dr.),
8) Podataka je činjenica na osnovu koje se oblikuje informacija,
9) Mjere informacijske sigurnosti su opća pravila zaštite informacijskog sustava na fizičkoj, tehničkoj i organizacijskoj razini,
10) Norma HRN EN ISO/IEC 27001:2023 je međunarodna norma ustanovljena da bi utvrdila zahtjeve za uspostavljanje, uvođenje, održavanje i trajno poboljšanje sustava upravljanja informacijskom sigurnošću,
11) Plan kontinuiteta poslovanja (BCP) je skup dokumentiranih postupaka za odgovor, oporavak, nastavak i vraćanje Agencije u stanje redovitog rada,
12) Upravljanje kontinuitetom poslovanja je proces koji omogućava Agenciji učinkovit odgovor i oporavak ključnih poslovnih procesa i usluga u slučaju njihovog iznenadnog i neželjenog prekida,
13) Poslovni proces je povezani skup aktivnosti i mjera koji se provodi radi ostvarenja cilja organizacije te uključuje sve one aktivnosti koje se moraju provesti između početne i krajnje točke kako bi se postigao željeni cilj,
14) Povjerljivost je svojstvo informacije da nije dostupna ili otkrivena neovlaštenim osobama,
15) Raspoloživost (dostupnost) je svojstvo informacije da je dostupna i upotrebljiva na zahtjev ovlaštenog korisnika,
16) Popis informacijske imovine je popis informacijske imovine Agencije koju treba adekvatno zaštititi od prijetnji i ranjivosti,
17) Rizik je mogući incident ili pojava koja nastaje iz unutarnjih ili vanjskih izvora, a koji može nepovoljno utjecati na ostvarenje ciljeva informacijske sigurnosti,
18) Vlasnik poslovnog procesa je voditelj ustrojstvene jedinice Agencije u kojoj nastaje, prikuplja se ili koristi dokumentacija odnosno informacije, a koji je ujedno i vlasnik poslovnih informacija nastalih u procesu te informatičkih sustava (programskog rješenja) koji se koriste u procesu,
19) Vlasnik informatičke opreme je voditelj ustrojstvene jedinice Agencije u čijoj nadležnosti je upravljanje informatičkom opremom i odgovoran je za organizaciju i ispravno funkcioniranje informatičkog sustava (IT tehnologije), a u skladu s usuglašenim zahtjevima s vlasnikom poslovnog procesa.

2. ULOGE, ODGOVORNOSTI I NADZOR

Članak 6.

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

- određuje ciljeve informacijske sigurnosti,
- osigurava resurse potrebne za upravljanje informacijskom sigurnošću,
- osigurava izvršavanje ciljeva upravljanja informacijskom sigurnošću i
- osigurava podizanje razine informacijske sigurnosti u Agenciji.

Članak 7.

Zaposlenik zadužen za uspostavu i nadzor informacijske sigurnosti 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,
- nadzire provedbu poslova zaštite informacijskog sustava,
- osigurava da svi zaposlenici Agencije budu upoznati s ovim Pravilnikom te nadzire provedbu trajne edukacije zaposlenika iz područja informacijske sigurnosti,
- nadzire vođenje jedinstvenog popisa informacijske imovine Agencije po poslovnim procesima i odgovoran je za njegovu povjerljivost, cjelovitost i raspoloživost,
- nadzire proces upravljanja rizicima informacijske imovine i prati realizaciju mjera za smanjenje rizika,
- u slučaju incidenata informacijske sigurnosti, nadzire provedbu analize uzroka incidenta uvidom u informacijski sustav Agencije i u druge izvore te o rezultatima podnosi izvještaj ravnatelju i
- najmanje jednom godišnje u postupku Upravine ocjene podnosi izvještaj o stanju informacijske sigurnosti.

Članak 8.

Pomoćnici ravnatelja i voditelji ustrojstvenih jedinica Agencije brinu se o provedbi mjera zaštite u poslovnim procesima koje nadziru te koje su ovlašteni organizirati, a u cilju zaštite cjelovitosti, autentičnosti i dostupnosti podataka te su odgovorni za:

- podršku i primjenu sustava upravljanja informacijskom sigurnošću u svom djelokrugu rada, osiguranje provedbe svih mjera zaštite u svom djelokrugu rada,
- provedbu kontinuirane procjene rizika informacijske sigurnosti unutar svojeg djelokruga rada, kao i redovno održavanje popisa informacijske imovine,
- organiziranje poslova u skladu s ovim Pravilnikom i pripadajućim standardnim operativnim postupcima,
- kontinuirano upoznavanje i osvještavanje zaposlenika o mjerama i standardima informacijske sigurnosti te nadzor nad radom zaposlenika,
- sudjelovanje u razvoju informacijskog sustava unutar svojeg djelokruga rada,
- koordinaciju provedbe mjera zaštite temeljenih na procjeni rizika informacijske sigurnosti i
- predlaganje novih mjera zaštite sustava informacijske sigurnosti.

Članak 9.

Vlasnik poslovnog procesa odgovoran je za informacije i funkcioniranje informacijskog sustava unutar procesa.

Neposredni vlasnik korisnik sklopovske imovine odgovoran je za pravilno korištenje opreme te čuvanje informacija sukladno ovom Pravilniku te općim aktima Agencije.

Zaposlenici su odgovorni za poznavanje i provedbu propisanih mjera i kontrola te suradnju u rješavanju incidenata informacijske sigurnosti u okviru svojih odgovornosti sukladno važećem općem aktu o unutarnjem ustrojstvu i sistematizaciji radnih mjesta u Agenciji.

Članak 10.

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

3. ZAŠTITA POVJERLJIVOSTI, CJELOVITOSTI I RASPOLOŽIVOSTI INFORMACIJA

Članak 11.

Agencija štiti povjerljivost, cjelovitost i raspoloživosti podataka i informacija poduzimanjem fizičkih, tehničkih, organizacijskih i drugih mjera zaštite sukladno općim aktima, politikama, Poslovnikom kakvoće i standardnim operativnim postupcima Agencije.

3.1. Razine povjerljivosti

Članak 12.

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

Članak 13.

Javne informacije su informacije koje Agencija javno objavljuje te one kojima je u određenim uvjetima omogućen pristup trećim osobama.

Članak 14.

Poslovno važne informacije su informacije koje su bitne za kontinuitet poslovanja i poslovne procese, a koriste ih zaposlenici Agencije u skladu s dodijeljenim ovlaštenjima.

Poslovno važne informacije i način postupanja s istima propisat će se Pravilnikom o tajnosti podataka.

Članak 15.

Interno tajnim informacijama se smatraju podaci u upravnim i neupravnim postupcima koje provodi Agencija na temelju zahtjeva fizičkih i pravnih osoba sukladno zakonskim i podzakonskim propisima koji propisuju područje lijekova, medicinskih proizvoda i veterinarskih lijekova, osobni podaci sukladno posebnom propisu, podaci koji su označeni kao poslovna tajna podnositelja zahtjeva kao i sve ostale informacije koje sadrže podatke utvrđene kao tajne Pravilnikom o tajnosti podataka.

Interno tajni podaci koji postaju javni završetkom upravnih i neupravnih postupaka propisat će se Pravilnikom o tajnosti podataka.

4. MJERE INFORMACIJSKE SIGURNOSTI

4.1. Mjere informacijske sigurnosti za područje fizičke sigurnosti

Članak 16.

Agencija na svim lokacijama na kojima obavlja djelatnost ili posjeduje imovinu provodi mjere višestruke zaštite fizičke sigurnosti radi smanjenja rizika i održavanja prikladne razine sigurnosti.

Provedba i organizacija mjera fizičke sigurnosti propisani se standardnim operativnim postupcima Agencije.

Članak 17.

Poslovni prostori i objekti Agencije, uključujući i prostore u kojima se nalazi oprema informacijskih sustava, kategoriziraju se u odnosu na pravo pristupa kao prostori posebne namjene ili kao ostali prostori.

Prostori posebne namjene u Agenciji moraju biti jasno označeni i dodatno zaštićeni sukladno propisanom standardnom operativnom postupku.

Kontrola osoba propisana je Pravilnikom o ulasku, izlasku i boravku u prostorima Agencije i provođenju sigurnosnih mjera.

Članak 18.

Neklasificiranih podaci u fizičkom obliku Agencije pohranjuju se u uredski namještaj koji se zaključava i u prostoru za otvorenu pohranu pod stalnom zaštitom i periodičnim nadzorom.

4.2. MJERE INFORMACIJSKE SIGURNOSTI ZA PODRUČJE SIGURNOSTI PODATAKA

Označavanje

Članak 19.

Agencija označava podatke koji se koriste isključivo u službene svrhe oznakom „Neklasificirano“.

Pristup podacima

Članak 20.

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

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

Pravo na pristup podacima i informacijskim sustavima, odnosno dijelovima informacijskog sustava Agencije dodjeljuje se u skladu s poslovnim potrebama i zahtjevima sigurnosti (ovlaštenja).

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

Članak 21.

Razina pristupa podacima i informacijskim sustavima ne smije biti viša od one koja je potrebna za obavljanje poslova i zadataka pripadajućih poslovnih procesa.

Najmanje jedanput godišnje vlasnici poslovnog procesa moraju provjeravati dana ovlaštenja.

Članak 22.

Upravljanje ovlaštenjima za pristup podacima i informacijskim sustavima, korisničkim računima i autorizacijama detaljnije se ureduje standardnim operativnim postupkom.

Zaštita podataka

Članak 23.

Zaštita podataka provodi se radi očuvanja njihove cjelovitosti, dostupnosti i povjerljivosti.

Mjere zaštite temelje se na upravljanju rizicima koje se detaljnije uređuju standardnim operativnim postupcima.

Postupanje u izvanrednim situacijama

Članak 24.

Radi osiguranja kontinuiteta poslovanja Agencija izrađuje Plan kontinuiteta poslovanja (BCP) kojim se utvrđuje postupanje u izvanrednim situacijama.

Način izrade plana kontinuiteta poslovanja uređuje se standardnim operativnim postupkom.

Mjere informacijske sigurnosti za područje zaštite informacijskih sustava

Zaštita hardvera, softvera i medija za pohranu podataka

Članak 25.

Zaštita informacijskog sustava temelji se na upravljanju rizicima, a upravljanje rizicima detaljnije je utvrđeno standardnim operativnim postupcima.

Mjerama zaštite informacijskog sustava Agencija štiti informatičku opremu, softver, medije za pohranu podataka i komunikacijsku opremu.

Mjere zaštite informatičke opreme, medija za pohranu i komunikacijske opreme uključuju zaštitu od neovlaštenog fizičkog pristupa, redovito održavanje ispravnog rada i zanavljanje i održavanje konfiguracije koja zadovoljava zahtjeve poslovnih procesa Agencije.

Članak 26.

Mjere zaštite softvera odnose se na zaštitu od neovlaštenog pristupa i izmjena, kontrole promjena, instaliranja tekućih sigurnosnih programskih zakrpa i zaštite od kibernetičkih napada.

Upravljanje sviješću o sigurnosti

Članak 27.

Upravljanje sviješću o sigurnosti podrazumijeva uspostavljanje sigurnosnih pravila te educiranje i stručno usavršavanje iz područja sigurnosti.

Članak 28.

Svi korisnici informacijskog sustava obvezni su primjenjivati utvrđena sigurnosna pravila koja su detaljno uređena standardnim operativnim postupcima.

Agencija provodi edukacije o informacijskoj sigurnosti i mogućim rizicima te obvezama i odgovornostima zaposlenika u vezi sa sigurnosnim aspektima uporabe informacijskog sustava.

Planiranje djelovanja u izvanrednim okolnostima

Članak 29.

U cilju osiguravanja kontinuiteta poslovanja, uspostavljaju se i testiraju procedure sigurnosne pohrane podataka, radi vraćanja sustava i podataka u prvobitno stanje nakon incidenta, kao što su kvarovi sustava, prirodne nepogode i kibernetički napadi te izrađuje Plan kontinuiteta poslovanja (BCP) kojim se utvrđuje postupanje u izvanrednim situacijama.

Način izrade plana kontinuiteta poslovanja uređuje se standardnim operativnim postupkom.

Članak 30.

Mjere zaštite informacijskog sustava Agencije detaljnije su utvrđene standardnim operativnim postupcima.

4.3. Mjere informacijske sigurnosti za područje poslovne suradnje

Ugovori s vanjskim pružateljem usluga i njegovim podizvođačima obvezno sadrži odredbe o poštivanju ili osiguravanju mjera zaštite informacijskog sustava Agencije.

Kada je za sklapanje ugovora o poslovnoj suradnji prethodno nužno omogućiti pristup informacijama, obvezno se sklapa sporazum o povjerljivosti kojim se druga strana obvezuje na poštivanje ili osiguravanje mjera zaštite informacijskog sustava.

Pristup informacijskom sustavu Agencije ne može se omogućiti prije početka važenja ugovora odnosno sporazuma o povjerljivosti.

5. UPRAVLJANJE RIZIKOM INFORMACIJSKE SIGURNOSTI

Članak 31.

Upravljanje rizikom informacijske sigurnosti sastoji se od trajnog procjenjivanja i obrade rizika, radi sprječavanja uništenja, otuđenja, gubitka i neovlaštenog pristupa podacima.

Članak 32.

Vlasnici poslovnih procesa upravljaju rizicima u svojim ustrojstvenim jedinicama te najmanje jednom godišnje ažuriraju popis informacijske imovine, procjenjuju rizike i analiziraju utjecaj rizika na poslovanje te odlučuju o mjerama za uklanjanje ili smanjenje rizika.

Upravljanje rizicima detaljnije je utvrđeno standardnim operativnim postupcima.

5.1. Incidenti

Članak 33.

Agencija 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 standardnim operativnim postupkom.

Svaki zaposlenik Agencije koji ima pristup informacijskoj imovini Agencije obvezan 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 obraduju se radi smanjenja vjerojatnosti ili negativnog učinka budućih incidenata.

5.2. Upravljanje kontinuitetom poslovanja

Članak 34.

Agencija 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 zaposlenika o načinima oporavka ključnih poslovnih procesa i aktivnosti.

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

U slučaju izvanrednih i kriznih situacija, postupa se prema planu i odlukama koje donosi ravnatelj Agencije, sukladno standardnom operativnom postupku.

Prijelazne i završne odredbe

Članak 35.

Agencija će se Pravilnik o tajnosti podataka u skladu s odredbom članka 14. ovoga Pravilnika donijeti u roku od 12 mjeseci od dana stupanja na snagu ovoga Pravilnika.

Članak 36.

Ovaj Pravilnik stupa na snagu osmog dana nakon objave na oglasnoj ploči Agencije za lijekove i medicinske proizvode.

KLASA: 025-02/26-02/03
URBROJ: 381-14-10/411-26-01

PREDSJEDNICA UPRAVNOG VIJEĆA

Davorka Herman Mahečić, dr.med.subspec.

AGENCIJA ZA LIJEKOVE I MEDICINSKE PROIZVODE 7 ZAGREB

HALMED

Agencija za lijekove i medicinske proizvode

Ovaj Pravilnik o provedbi mjera i standarda informacijske sigurnosti Agencije za lijekove i medicinske proizvode objavljen je na oglasnoj ploči Agencije za lijekove i medicinske proizvode dana 04. ožujka 2026. godine te je stupio na snagu dana 12. ožujka 2026. godine.

RAVNATELJ

Prof. dr. sc. Siniša Tomić