Na podlagi 2. alineje prvega odstavka 11. člena Sklepa o ustanovitvi Javne agencije RS za zdravila in medicinske pripomočke (Uradni list RS, št. 115/06 in 70/17), za izvajanje Uredbe o informacijski varnosti v državni upravi (Uradni list RS, št. 29/18 in 131/20), po predhodni pridobitvi mnenja Sindikata državnih organov Slovenije z dne 13.9.21021 in mnenja Sindikata farmacevtov Slovenije z dne 10.9.2021 je Svet Javne agencije Republike Slovenije za zdravila in medicinske pripomočke na svoji 28. redni seji, dne 18. 11. 2021, sprejel naslednji:

PRAVILNIK O INFORMACIJSKI VARNOSTNI POLITIKI
JAVNE AGENCIJE REPUBLIKE SLOVENIJE
ZA ZDRAVILA IN MEDICINSKE PRIPOMOČKE

SPLOŠNE DOLOČBE

1. člen

S tem pravilnikom se določa informacijska varnostna politika (v nadaljevanju: IVP) Javne agencije Republike Slovenije za zdravila in medicinske pripomočke (v nadaljevanju: agencija).,

2. člen

Ta pravilnik morajo upoštevati vodstvo, zaposleni, osebe pogodbenih izvajalcev in vsi, ki imajo dostop do informacijskega premoženja agencije.

3. člen

Namen IVP je postaviti osnovna varnostna izhodišča za zaščito informacijskih sredstev pred nevarnostmi, bodisi notranjimi ali zunanjimi, namernimi ali naključnimi. Izvajanje te politike je pomembno za zagotavljanje informacijske varnosti.

Informacijsko varnost označujemo kot varovanje:
- **zaupnosti**: varovanje podatkov in informacij pred razkritjem nepooblaščenim osebam ter zagotavljanje odgovornosti za njihova dejanja;
- **celovitosti**: varovanje podatkov in informacij pred neavtoriziranimi spremembami, zagotavljanje verodostojnosti – točnosti, popolnosti in nespremenljivosti informacij ter postopkov procesiranja;
- **razpoložljivosti**: varovanje podatkov, informacij in servisov pred prekinitvami v delovanju ter zagotavljanje informacij pooblaščenim uporabnikom v času, ko jih potrebujejo, in na zahtevani način.

4. člen

Z IVP se zagotavlja doseganje naslednjih temeljnih ciljev:
- zavarovanje podatkov in informacij pred nepooblaščenim dostopom, obdelavo ter razkritjem,
- ohranitev celovitosti informacij in preprečevanje nepooblaščenih sprememb,
- razpoložljivost informacij in virov, ko jih pooblaščene osebe potrebujejo,
- izobraževanja o informacijski varnosti,
- beleženje in raziskovanje kršitev IVP in sum teh kršitev,

- preverjanje skladnosti z zakonodajo,
- upoštevanje priporočil glede standardov informacijske varnosti.

5. člen

Izrazi v tem pravilniku imajo naslednji pomen:

1. **aplikacija** – programska oprema, ki nudi informacijsko podporo za izvajanje procesov JAZMP, omogoča sprotno ali obdobno izmenjevanje podatkov med agencijo in drugimi poslovnimi subjekti;
2. **elektronska pošta** – storitev za izmenjavo elektronskih sporočil;
3. **elektronski poštni predal** – zbirka podatkov, v kateri se shranjujejo elektronska sporočila uporabnika ali namenske skupine uporabnikov, prejeta ali poslana po sistemu elektronske pošte;
4. **elektronsko sporočilo** – niz podatkov, ki so poslani ali prejeti po elektronski poti;
5. **enota za IT** – zaposleni v organizacijski enoti, ki nudi informacijsko podporo agenciji;
6. **incident** – dogodek, katerega posledica je razkritje, uničenje, nerazpoložljivost podatkov ali informacijskega sistema in kršitev varnostne politike;
7. **informacijski sistem** – celoten skupek opreme (komunikacijske in informacijske) in postopkov za obravnavanje podatkov agencije;
8. **informacijski varnostni dogodek** – stanje ali sprememba, ki lahko vpliva na varnost podatkov v informacijskem sistemu ali na delovanje informacijskega sistema;
9. **infrastruktura –** energetski in komunikacijski vodi, generatorji, klimatske naprave, sistemi neprekinjenega napajanja (sistemi UPS), sistemi za gašenje, prostori, …;
10. **izmenljivi nosilci podatkov** – nosilci podatkov, ki jih je mogoče z enostavnim posegom odstraniti in ločiti od informacijskega sistema. Sem sodijo CD in DVD mediji, USB-pomnilniki in diski;
11. **nepooblaščeni dostop** – nedovoljen dostop do prostorov, podatkov in informacij, dostop brez ustreznega pooblastila;
12. **nosilec podatkov** – priprava ali sredstvo, ki omogoča branje in/ali zapisovanje podatkov (CD, DVD, disk, USB-pomnilnik, kartica, trak, kaseta, papir, …);
13. **obravnavanje podatkov** – zbiranje, obdelava, prikaz, hranjenje, spreminjanje in brisanje podatkov;
14. **ocena tveganja** – ugotovitev vseh morebitnih tveganj in nevarnosti, ki lahko ogrozijo varnost in poslovanje agencije;
15. **pooblaščena oseba** – posameznik ali skupina ljudi, imenovana na podlagi zakona ali s strani direktorja za izvajanje določenih nalog;
16. **skrbnik** – pooblaščena oseba, odgovorna za upravljanje posameznega sistema ali podsistema (načrtov, procesov, opreme, infrastrukture, informacijske varnosti, informacijskega sistema, …) ali aplikacije;
    a. **informacijski skrbnik aplikacije** – informatik, ki organizira tehnično izvedbo nalog;
    b. **vsebinski skrbnik aplikacije** – delavec s področja poslovanja, katerega procese aplikacija podpira in ki dodeljuje uporabniške pravice, predlaga spremembe, nadgradnje in zagotavlja pravilnost uporabe aplikacije. Je dober poznavalec poslovnih procesov in podatkov tega področja;
17. **sredstva za dostop do informacijskega sistema** – uporabniško ime in geslo, pametne kartice, certifikati, enkratna gesla in drugi načini za avtentikacijo in avtorizacijo uporabnikov informacijskega sistema;
18. **svetovni splet** – internet, medmrežje;

19. **šifriranje** – preoblikovanje razumljivega besedila v nerazumljivo obliko s kriptografskimi metodami;
20. **uporabnik** – oseba, ki uporablja informacijski sistem ali napravo pri rednem delu in ima sklenjeno pogodbo o zaposlitvi oziroma je v delovnem razmerju na agenciji ali je zunanji pogodbeni izvajalec agencije;
21. **uporabniško ime in geslo** – niz znakov, s katerim se uporabnik prijavi v informacijski sistem;
22. **upravljanje** – zajem funkcij, kakršne so načrtovanje, montaža, zagotavljanje, obratovanje, administriranje in vzdrževanje sistema;
23. **varnostne kopije** – so prepisi točno določenih podatkov, da se zavarujejo pred izgubo, in so navadno prepisani na optično ali magnetno sredstvo;
24. ;
25. **zaupni podatki** –, osebni podatki, poslovne skrivnosti, drugi podatki, ki jih kot zaupne določa zakon ali jih kot takšne opredeli direktor agencije oziroma od njega pooblaščena oseba;
26. **zunanji izvajalec** – vsaka fizična ali pravna oseba, ki dobavi opremo ali izvaja storitve po pogodbi za agencijo.

6. člen

V informacijskem sistemu mora biti zagotovljeno zaznavanje kršitev IVP na način, da je omogočeno njihovo sankcioniranje po veljavni zakonodaji ali pogodbi.

Glede na interes agencije se lahko uporabijo tudi drugi ukrepi. Agencija ima pravico do takojšnje blokade in morebitne naknadne ukinitve storitve, če ugotovi kršitev določb IVP.

7. člen

Sistemi v lasti in upravljanju agencije, povezani z internetom, intranetom ali ekstranetom, poleg ostalega obsegajo računalniško strojno opremo, programsko opremo, operacijske sisteme, uporabniške račune za elektronsko pošto, brskanje po spletu in prenos datotek. Omenjeni sistemi se uporabljajo za poslovne namene agencije in ob normalnem delovanju služijo izključno interesom agencije in strankam ter poslovnim partnerjem agencije.

8. člen

Uporabniki se morajo zavedati, da so vsi podatki, ki se kreirajo na sistemih v lasti agencije, last agencije, razen podatkov iz zasebne sfere zaposlenih, ki so jih kreirali zaposleni sami in za obdelavo katerih agencija nima pravne podlage v zakonodaji. Zaradi potrebe po zaščiti informacijskega okolja agencije vodstvo ne more zagotavljati zaupnosti zasebnih informacij, shranjenih na katerem koli sistemu, ki pripada agenciji.

Zaposleni so odgovorni za razumno in sprejemljivo rabo informacijskih sredstev za zasebne namene.

FIZIČNO VAROVANJE

Varovanje prostorov

9. člen

Prostori, v katerih se obdelujejo in obravnavajo podatki, morajo biti varovani z organizacijskimi, fizičnimi in tehničnimi ukrepi, ki nepooblaščenim osebam onemogočajo dostop do informacijske in komunikacijske tehnologije za obdelavo podatkov.

V poslovnem času agencije fizično in tehnično varovanje notranjih in zunanjih prostorov izvaja varnostna služba, s katero ima agencija sklenjeno pogodbo. Obiskovalci agencije se morajo obvezno javiti pri recepciji in varnostniku povedati, h komu so prišli in s kakšnim namenom.

Obiskovalci praviloma ne vstopajo v delovne prostore agencije, ampak so temu namenjene skupne komunikacijske in sejne površine.
Posamezne delovne prostore po končanem delovnem času zaklenejo zaposleni.

Varovanje sredstev za dostop

10. člen

Vsak zaposleni na agenciji mora fizična sredstva (ključi, registracijske kartice itd.) in elektronska sredstva (uporabniška imena, gesla, šifrirni ključi itd.) za dostop do prostorov, podatkov in opreme varno in skrbno hraniti, jih imeti vedno pod nadzorom in jih ne sme posojati.

Varovanje opreme

11. člen

Vsa oprema mora biti nameščena in zaščitena tako, da so nevarnosti iz okolja in priložnosti za nepooblaščeni dostop kar najbolje odpravljene.

Raven varovanja in zaščite je odvisna od zaupnosti podatkov in ocenjenega tveganja izgube ali poškodovanja podatkov. Zahtevo za morebitno posebno varovanje podatkov poda vsebinski skrbnik aplikacije.

12. člen

Protipožarno varovanje na območjih, na katerih je nameščena ključna ali pomožna oprema, mora biti izvedeno skladno s predpisi in navodili pooblaščenih služb.

13. člen

Ožičenje podatkovnega omrežja morajo vedno načrtovati in nameščati usposobljeni izvajalci. Izvedeno mora biti skladno z veljavnimi standardi in predpisi.

Varnost ožičenja podatkovnega omrežja je treba načrtovati že pri načrtovanju računalniških prostorov in namestitve opreme. Pri vsaki nadgradnji ali spremembi omrežja ali vanj vključenih naprav mora biti preverjena varnost ožičenja.

Električni in telekomunikacijski kabli (ožičenje), po katerih se prenašajo podatki oziroma ki podpirajo informacijske storitve, morajo biti zaščiteni pred prestrezanjem ali poškodbami.

14. člen

Uporabniki morajo vsako okvaro in namerno ali nenamerno poškodbo opreme sporočiti enoti za IT, ki ukrepa glede na težo in vrsto okvare.

15. člen

Agencija vzdržuje evidenco vse informacijske opreme, ki je s strani agencije dodeljena v uporabo zaposlenim.

Evidenca opreme mora vsebovati podatke o vrsti, proizvajalcu, tipu, serijski številki, uporabniku in datumu začetka uporabe opreme..

INFORMACIJSKA VARNOST

Vloge in odgovornosti

16. člen

Za izvajanje posameznih ključnih nalog na področju informacijske varnosti v agenciji direktor določi osebo, zadolženo za upravljanje sistema informacijske varnosti (v nadaljevanju: koordinator informacijske varnosti).

Koordinator informacijske varnosti na področju informacijske varnosti izvaja naloge, ki obsegajo:
- zagotavljanje varnega izbrisa ali uničenja nosilcev podatkov,
- odzivanje in obravnavo incidentov informacijske varnosti v agenciji,
- zagotavljanje usposabljanja in ozaveščanja na področju informacijske varnosti,
- poročanje direktorju v zvezi s stanjem informacijske varnosti agencije,
- odobri prenos programske oziroma strojne opreme v obratovalno okolje.

Uporaba opreme informacijske tehnologije

17. člen

Informacijska oprema v lasti agencije je namenjena opravljanju dela oziroma potrebam dela v sklopu delovnega procesa agencije.

Uporaba v zasebne namene ni dovoljena, razen v obsegu, ki ne moti delovnega procesa in varnosti.

18. člen

Uporabniki morajo z informacijsko opremo agencije ravnati kot dober gospodar, po priporočilih in navodilih proizvajalca ter skrbnika sistema. Posege vanjo lahko opravljajo samo za to pooblaščene osebe.

Za odtujitev in poškodbe opreme je odgovoren uporabnik. Posebno skrbno mora ravnati s prenosno opremo.

Na informacijski opremi agencije v skupni rabi uporabniki ne shranjujejo zasebnih multimedijskih datotek (fotografije, glasba, filmi ipd.) in piratskih kopij del, zaščitenih z zakonom, ki ureja avtorsko in sorodne pravice.

Če se nahajajo na lokalnem disku računalnika, ki ni v skupni rabi, zasebne datoteke, jih je uporabnik dolžan sproti odstranjevati.

Prepovedano je obremenjevati delovanje informacijskega sistema s podatki iz zasebne sfere zaposlenih, ki so jih kreirali zaposleni sami.

19. člen

Enota za IT izvaja varnostno kopiranje informacijskega sistema. S tem zagotavlja, da se zmanjša možnost iz izgube informacij, ki so pomembne za poslovanje agencije.

Koordinator informacijske varnosti vodi načrt varnostnih kopij, ki vsebuje podatke o obsegu, pogostosti, času in načinu hranjenja varnostnih kopij.

20. člen

Namen uporabe tiskalnikov in multifunkcijskih naprav je izvajanje delovnega procesa za zaposlene na agenciji.

Izjemoma lahko zaposleni na agenciji uporabljajo tiskalnike in multifunkcijske naprave tudi za zasebne namene, vendar v obsegu, ki ne ovira izvajanja delovnega procesa za zaposlenega in za druge uporabnike.

Enota za IT zagotavlja nadzorni sistem, kjer je razvidna količina natisnjenih ali kopiranih strani na tiskalnikih oziroma multifunkcijskih napravah na uporabnika v določenem časovnem obdobju.

Direktor lahko določi največjo dovoljeno količino natisnjenih ali kopiranih strani v določenem časovnem obdobju na tiskalnikih oziroma multifunkcijskih napravah. V primeru preseganja največje dovoljene količine mora zaposleni izkazati utemeljenost tiskanja ali kopiranja.

21. člen

Uporabniki lahko nameščajo programsko opremo samo z dovoljenjem skrbnikov informacijskih sistemov.

Zlonamerna programska oprema

22. člen

Nameščanje ali uporaba zlonamerne programske opreme ali njeno širjenje je kršitev IVP.

Namerno nameščanje, uporaba in širjenje take opreme se obravnava v skladu z veljavno zakonodajo.

Uporabniki:
- morajo, če sumijo, da na informacijskem sistemu deluje zlonamerna programska oprema, takoj nehati delati z njim, obvestiti pristojno osebo in upoštevati njena navodila;
- morajo, če sumijo, da je na informacijskem sistemu zlonamerna programska oprema, takoj obvestiti pristojno osebo in upoštevati njena navodila;
- ne smejo zaganjati izvršljive programske kode, ki ni del njihovega informacijskega sistema (izvira npr. s svetovnega spleta, elektronske pošte, pomnilniških medijev);
- ne smejo zaganjati dokumentov (npr. s svetovnega spleta, elektronske pošte, pomnilniških medijev), če so sumljivi, če ne vedo, čemu so takšni dokumenti ali programi namenjeni, ali če ne poznajo njihovega izvora;
- morajo, če sumijo ali ugotovijo, da sistem za protivirusno zaščito ne deluje ali ni ustrezno posodobljen, takoj nehati uporabljati informacijski sistem, obvestiti skrbnika in upoštevati njegova navodila.

Informacijski sistemi

23. člen

Informacijski sistemi, ki obravnavajo zaupne podatke, morajo biti nadzorovani.

Nadzirajo se lahko tudi sistemi, ki obravnavajo druge podatke. V nadzorovanih sistemih morajo biti vključeni dnevniki, ki zagotavljajo spremljanje dogodkov. Dnevniki morajo omogočiti identifikacijo uporabnika.

Izpis ali izvoz podatkov iz dnevnikov mora ostati pod nadzorom in nespremenjen. Podatke iz dnevnika, ki niso prosto dostopni, je mogoče pridobiti le na pisno zahtevo direktorja ali na zahtevo pristojnega preiskovalnega organa v zvezi s sumom storitve kaznivega dejanja.

Podatki iz dnevnika se uporabljajo tudi za odkrivanje napak v informacijskem sistemu ali za izboljšanje njegovega delovanja. Če dnevniki vsebujejo zaupne podatke, morajo biti zabeleženi vpogledi v dnevnike.

24. člen

Priključitev zasebne opreme v interno omrežje agencije ni dovoljena.
Zasebna oprema se lahko priključi v omrežje v upravljanju agencije, ki je namenjeno obiskovalcem.

Upravljanje izmenljivih nosilcev podatkov

25. člen

Izmenljivi nosilci podatkov neznanega ali sumljivega izvora se ne smejo uporabljati. Preden se uporabi vsebina izmenljivega nosilca podatkov, se mora vselej preveriti njegova morebitna okuženost z zlonamerno programsko opremo.

26. člen

Uporabnik mora nosilce podatkov z zaupnimi podatki, ki jih ne potrebuje več oziroma so neuporabni, izročiti skrbniku.

Dostop do informacijskih sistemov

27. člen

Dostop do storitev in upravljanja informacijskih sistemov ter omrežja je urejen po sistemu pravic. Te dodeljuje skrbnik informacijskega sistema ali omrežja.

Na podlagi potreb poslovnega procesa se odobri dostop do informacijskega sistema v obsegu, potrebnem za opravljanje delovnih nalog.

Dostop do posameznih informacijskih sistemov in njegovih delov smejo imeti samo osebe, ki so do tega upravičene, za to pooblaščene in usposobljene.

28. člen

Dostop do informacijskih sistemov agencije mora biti omogočen le na podlagi ustrezne avtentikacije, minimalno z uporabo uporabniškega imena in gesla. Za prijavo v sistem se lahko poseže še po drugih odobrenih avtentikacijskih metodah.

29. člen

Za vsak sklop informacijskega sistema agencije mora skrbnik zadevnega sklopa informacijskega sistema določiti dodelitve, spremembe in odvzem dostopnih pravic zaposlenim.

Pravico dostopa do sklopov informacijskega sistema lahko pridobijo uporabniki ali administratorji na podlagi potrebe in odobritve skrbnika sklopa informacijskega sistema. Če potreba po dostopu preneha, je treba to pravico odvzeti.

Postopek upravljanja pravic dostopa do sklopov informacijskega sistema mora biti dokumentiran, dodeljene pravice pa redno pregledovane.

Skrbniki sklopov informacijskega sistema morajo poskrbeti, da so sklopi informacijskih sistemov ustrezno posodabljani.

30.

31. člen

Uporabniške in administratorske pravice dostopa do informacijskih sistemov so ločene.

Načelo čiste mize

32. člen

Uporabniki ne smejo puščati nosilcev podatkov (npr. v papirni obliki, elektronskih medijev) z zaupnimi podatki na odprtih površinah pisarniške opreme ali drugih mestih, kjer bi lahko bili dostopni nepooblaščenim osebam. Ko uporabnikov ni v prostoru, morajo biti nosilci podatkov varno shranjeni. Zunaj delovnega časa mora biti vsa pisarniška oprema, kjer se hranijo nosilci podatkov, ki niso javni, zaklenjena ali drugače varovana, komunikacijsko-informacijska oprema pa fizično ali programsko varovana.

Načelo praznega zaslona

33. člen

Ob uporabnikovi prisotnosti ali odsotnosti na delovnem mestu mora biti onemogočen vpogled na zaslon oziroma onemogočena uporaba informacijsko-komunikacijske opreme nepooblaščenim osebam:

- delovna mesta morajo biti v okviru možnosti organizirana tako, da se prepreči priložnostno "gledanje čez rame";
- uporabljati se mora oprema in nastavitve, ki po določenem času uporabnikove neaktivnosti na delovni postaji izključijo zaslon ali ga preklopijo na ohranjevalnik zaslona, zavarovan z geslom;
- ob vsaki zapustitvi delovnega mesta je treba zakleniti ekran;
- ob koncu delovnega procesa se je treba odjaviti iz sistema in izklopiti delovno postajo, razen če ni z drugim navodilom določeno drugače.

Oddaljeni dostop

34. člen

Oddaljeni dostop do informacijskega sistema je dovoljen le na podlagi odobrene metode z ustrezno ravnjo varnosti, in sicer za tiste uporabnike, ki dostop potrebujejo zaradi opravljanja delovnih nalog. Treba je upoštevati tudi načelo praznega zaslona.

Po končanem delu se je treba odjaviti iz sistema in zagotoviti, da zaupni podatki in sledi ne ostanejo na delovni postaji.

35. člen

Ko se pojavi potreba po dostopu tretjih strank do informacij ali informacijskega sistema agencije, se najprej izvede analizo tveganja in ugotovi potrebne varnostne ukrepe. Dostop tretjim strankam do informacij ali informacijskega sistema ni dovoljen, dokler niso implementirani ustrezni varnostni in nadzorni mehanizmi in ni stopila v veljavo pogodba, ki definira pogoje dostopa.

Tretjim strankam se omogoči dostop samo do tistih informacij in sistemov, ki jih nujno potrebujejo pri svojem delu oziroma izpolnjevanju pogodbenih obveznosti, da se zmanjšujejo možnosti za nepooblaščen dostop.

Če se pojavi sum kršitve varnostnih predpisov in navodil, se dostop v omrežje začasno onemogoči, dokler se ne ugotovi dejanskega stanja kršitve.

Dostop do svetovnega spleta in storitev v svetovnem spletu

36. člen

Dostop do svetovnega spleta je omogočen zaposlenim za njihovo delo, izobraževanje in informiranje.

Zaposleni na agenciji morajo uporabljati svetovni splet v skladu z etičnimi in moralnimi normami. Zaposlenim na agenciji ni dovoljeno širjenje ali dostopanje do žaljivih in neprimernih ali nezakonitih vsebin.

Svetovni splet je sprejemljivo uporabljati v zasebne namene le v obsegu, ki ne ovira delovnega procesa, in na način, ki ne ogroža varnosti informacijskega sistema.

Vsi uporabniki informacijskih sistemov agencije se morajo zavedati, da se v medmrežju izkazujejo z mrežnim naslovom agencije kot pravne osebe javnega prava.

37. člen

Za zagotavljanje informacijske varnosti in razpoložljivosti informacijskih virov, zaradi preprečevanja kršitev etičnih in moralnih norm ter zaradi nemotenega poteka delovnega procesa, je mogoče tudi omejevati dostop do vsebin.

Direktor lahko določi spletne naslove ali vsebine, do katerih se bo tehnično omejil dostop.

38. člen

Pošiljanje službenih elektronskih naslovov na zunanje spletne strežnike ni dovoljeno, razen če je povezano s poslovnim procesom agencije.

39. člen

V omrežju agencije se lahko z namenom preiskave suma nezakonitih dejanj beležijo dostopi uporabnikov do spletnih storitev in s tem povezani podatki o dodeljenih internih IP številkah, času dodelitve interne IP številke ter podatki o povezavi med interno in javno IP številko. Te podatke lahko skrbniki sistema posredujejo le na obrazloženo zahtevo organa, ki na podlagi zakonskih pooblastil obravnava domnevno nezakonita dejanja.

Obdelava podatkov v nasprotju s prvim odstavkom tega člena ni dovoljena. Podatki se hranijo največ 1 leto.

ELEKTRONSKA POŠTA

40. člen

Zaposleni na agenciji kot orodje za komunikacijo s strankami, zaposlenimi, zunanjimi izvajalci ter drugimi deležniki uporabljajo tudi elektronsko pošto in poštni strežnik agencije. Pri tem se morajo držati ne le etičnih in moralnih norm, temveč tudi bontona. Vsebina elektronske pošte ne sme vsebovati neprimerne ali žaljive vsebine, ki bi škodila ugledu agencije.

Pošiljatelj se mora zavedati, da se vsako elektronsko sporočilo s službenega elektronskega naslova pri prejemniku lahko razloži kot mnenje agencije.

41. člen

Sistem elektronske pošte agencije se praviloma uporablja samo v službene namene. Uporaba v druge namene je dopustna le izjemoma, če ne moti delovnega procesa in varnosti (zaupnost, celovitost in razpoložljivost) informacijskega sistema.

42. člen

Uporabniki po elektronski pošti ne smejo pošiljati verižnih pisem in obsežnih datotek (glasba, filmi, predstavitve, zagonske datoteke in literatura), razen če so namenjene delu.

Sumljivo pošto naj zaposleni posredujejo izključno skrbnikom informacijskega sistema oziroma enoti za IT.

43. člen

Uporabniki svojega službenega elektronskega naslova ne smejo uporabljati v trženjske namene in z njega ne smejo pošiljati oglasne pošte na znane in/ali neznane naslove ter ustvarjati piramidnih shem.

44. člen

Pri posredovanju ali vračanju elektronske pošte (»Posreduj«, »Odgovori« in »Odgovori vsem«) morajo biti uporabniki previdni in preveriti, ali je pošta naslovljena na prave naslove. Predhodna korespondenca in varovani osebni podatki naj se v teh primerih brišejo, razen v utemeljenih primerih, ko je to potrebno zaradi narave delovnega procesa.

Zaposleni se ne smejo prijavljati na oglasno pošto ali novice z elektronskimi naslovi agencije, razen če to ni povezano s potrebami delovnega mesta.

45. člen

Uporabniki morajo biti previdni pri odpiranju pošte s priponkami, ki je bila prejeta od neznanih pošiljateljev. Če sumijo, da gre za neželeno pošto, ki bi bila lahko škodljiva, naj je ne odpirajo, temveč naj o tem obvestijo skrbnika poštnega sistema.

46. člen

Elektronsko pošto in priponke, ki vsebujejo zaupne podatke, je treba pri pošiljanju v zunanje omrežje po elektronski pošti šifrirati.

47. člen

S službenimi elektronskimi sporočili je treba ravnati v skladu z veljavnimi pravili poslovanja z dokumentarnim gradivom. Elektronska komunikacija, ki predstavlja evidenčno gradivo, se pokniži v dokumentni sistem.

Za prijavo na dogodke in za sporočila, povezana z opravljanjem delovnih nalog, ni dovoljeno uporabljati zasebnih elektronskih naslovov. Službene elektronske pošte ni dovoljeno preusmerjati na druge zasebne naslove.

Pravice nad podatki elektronske pošte

48. člen

Uporabniki se morajo zavedati, da se elektronska sporočila v sistemu elektronske pošte varnostno shranjujejo in bodo ostala shranjena tudi, če jih uporabniki izbrišejo iz svojega elektronskega poštnega predala.

Uporabniki se morajo zavedati, da elektronsko pošto lahko, odvisno od tehnologije, prestrežejo in obdelujejo nepooblaščene osebe.

49. člen

Uporabnik ne sme uporabljati elektronskega poštnega naslova, ki je bil dodeljen drugemu uporabniku.

50. člen

Pošiljateljem elektronskih sporočil na ukinjeni elektronski poštni naslov se pošlje sporočilo o nedostopnosti elektronskega poštnega naslova. Sprejemanje elektronskih sporočil na ukinjeni elektronski poštni naslov se onemogoči. Preusmeritev elektronske pošte v poštni predal drugega uporabnika ni dovoljena.

51. člen

Elektronska sporočila, ki jih prejme uporabnik na svoj elektronski poštni naslov, sme odpirati samo ta uporabnik ali s strani uporabnika pisno pooblaščena oseba, drug uporabnik pa samo na podlagi odredbe pristojnega državnega organa ali v izjemnih primerih (nenadna odpoved delavca, smrt delavca, ali drug izreden dogodek) komisijsko na podlagi sklepa direktorja, če je to neizogibno nujno potrebno za vodenje delovnega procesa. Pri tem se morajo upoštevati določbe veljavne zakonodaje.

52. člen

V primeru izjemnega primera iz prejšnjega člena vpogled v vsebino elektronske pošte zaposlenega v agenciji opravi tričlanska komisija, ki jo vsakokrat s sklepom imenuje direktor. V njej mora biti vsaj en predstavnik zaposlenih v agenciji, ki ni direktor ali vodja sektorja. O vpogledu mora komisija napisati zapisnik. Vpogled se skladno z načelom sorazmernosti omeji na ciljano vsebino, zaradi katere se vpogled izvaja.

O možnosti vpogleda iz prvega odstavka tega člena mora biti oseba, v elektronsko pošto katere se vpogleduje, predhodno pisno obveščen, razen ko to ni mogoče.

53. člen

Elektronska sporočila, ki prihajajo na skupne namenske elektronske poštne naslove (npr. glavna pisarna, info naslov, ipd.), odpirajo za to pooblaščene osebe.

Privzete nastavitve predala

54. člen

Uporabnik ne sme spreminjati privzetih nastavitev svojega elektronskega poštnega predala. Za uporabo dodatnih pripomočkov mora pridobiti posebno dovoljenje oziroma odobritev skrbnika.

Velikost elektronskih sporočil

55. člen

Največja velikost elektronskih sporočil pri pošiljanju ali sprejemanju elektronske pošte skupaj s priponko med posameznimi sistemi elektronske pošte je praviloma omejena. Če je omejitev presežena, se elektronsko sporočilo samodejno zavrne, pošiljatelj pa dobi obvestilo o zavrnitvi.

Dovoljeno največjo velikost priponke se lahko omeji glede na razpoložljive računalniške vire in potrebe delovnega mesta zaposlenega z namenom preprečiti izpad storitve elektronske pošte. Prav tako se lahko omeji število prejemnikov posameznega elektronskega sporočila.

56. člen

Če uporabnik prejme elektronsko sporočilo, ki ni namenjeno njemu, vsebine tega elektronskega sporočila ne sme shraniti ali kakor koli uporabiti. O tej pomoti mora obvestiti pošiljatelja, elektronsko sporočilo pa mora nemudoma izbrisati.

Brisanje elektronskih sporočil

57. člen

Vsak uporabnik mora vsa elektronska sporočila, ki jih ne potrebuje več, občasno brisati iz svojega predala oziroma mora to storiti na zahtevo skrbnika informacijskega sistema. Pri shranjevanju elektronskih sporočil morajo uporabniki upoštevati načelo racionalnosti in se izogibati hranjenju dokumentov v multimedijskih podatkovnih formatih, ki zavzamejo veliko prostora (filmi, slike visoke resolucije, zvočni zapisi).

Elektronska sporočila, ki so zasebne narave, morajo uporabniki brisati sproti.

Elektronski poštni predali nekdanjih zaposlenih

58. člen

Elektronski poštni predal zaposlenega se ob prenehanju delovnega razmerja briše.

Posebna pooblastila

59. člen

Za varno in nemoteno delovanje sistema elektronske pošte skrbi enota za IT.

Ob sumu storitve kaznivega dejanja z uporabo elektronskih sporočil se po odredbi pristojnega državnega organa opravijo postopki skladno z veljavno zakonodajo. Pregledovanje elektronskih sporočil iz radovednosti ali po nalogu nepooblaščenih posameznikov ni dovoljeno.

60. člen

V informacijskem sistemu agencije se izdelujejo in hranijo varnostne kopije.

Vsebinski skrbniki aplikacij in podatkov vsaj enkrat letno preverijo v enoti za IT, če je podatke v varnostnih kopijah mogoče pravilno restavrirati.

Pred prenosom vsakega novega sklopa informacijskega sistema v produkcijsko okolje mora zunanji izvajalec, ki je pripravil informacijsko rešitev, pripraviti navodila za izdelavo, hrambo in preverjanje varnostnih kopij podatkov, ki jih ta obravnava.

Ozaveščanje in usposabljanje

61. člen

Koordinator informacijske varnosti zagotovi sprotno seznanjanje zaposlenih z vsebino s področja informacijske varnosti.

Zaposlenim, ki opravljajo naloge razvoja in upravljanja informacijskih sistemov, je treba poleg splošnih usposabljanj s področja informacijske varnosti omogočiti tudi usposabljanje na specifičnih področjih informacijske varnosti glede na naloge, ki jih opravljajo.

Obvladovanje incidentov informacijske varnosti

62. člen

Med incidente informacijske varnosti sodijo:

- kibernetski napadi (vdori v omrežje, DDoS napadi, načrten zagon zlonamerne kode),
- odkritje zlonamerne programske kode na programski ali strojni opremi ali sumljivo vedenje opreme,
- izguba ali kraja informacijskega premoženja agencije,
- človeške napake (nepooblaščeno razkritje informacij),
- okvara strojne opreme, ki ima za posledico ogrožanje zaupnosti, dostopnosti ali celovitosti podatkov,
- odkritje ranljivosti, ki poveča možnost katerega od navedenih dogodkov.

63. člen

Zaposleni na agenciji in pogodbeni izvajalci so dolžni poročati o incidentu informacijske varnosti koordinatorju informacijske varnosti nemudoma ob odkritju incidenta.

Zaposleni ne smejo raziskovati ali samostojno izvajati ukrepov.

64. člen

Koordinator informacijske varnosti vodi evidenco incidentov, v kateri se vodijo podatki o časovni razpon incidenta, opis, sklope vpletenih informacijskih sistemov, morebitnem velikem tveganju za pravice in svoboščine posameznikov ter obveščenih osebah.

O incidentu koordinator informacijske varnosti naredi zapis, v katerem se vodijo podatki o:

- časovnem razponu incidenta,
- opisu incidenta,
- informacijskih sistemih, ki so ob incidentu prizadeti,
- zavarovanih dokazih,
- opisu reševanju incidenta,
- vzrokih za incident in povzročiteljih incidenta,
- izvedenih aktivnostih za odpravo posledic incidenta,
- stroških odprave in obnove po incidentu,
- nadaljnjih aktivnostih,
- negativnih poslovnih učinkih (nepooblaščeno razkritje informacij, nepooblaščena sprememba, nerazpoložljivost, uničenje, drugo),
- subjektih, obveščenih o incidentu.

Koordinator informacijske varnosti lahko za izvajanje ukrepov odziva na dogodke informacijske varnosti izvaja naslednje tehnične ukrepe:

- izolacija kompromitiranega segmenta omrežja, storitev ali naprav, zlasti s preklicem certifikata naprave, izključitvijo iz domene, onemogočenim uporabniškim računom, logičnim onemogočenjem komunikacije preko usmerjevalne naprave ali požarne pregrade, izklopom naprave ali storitve,
- uničenje podatkov na lokalnih napravah, zlasti zlonamerne kode, kompromitirane uporabniške račune, gesla in ključe,
- utrjevanje omrežja, naprav in storitev, zlasti z onemogočanjem neuporabljenih vlog, datotek in storitev, zapiranjem poti komunikacije, implementacijo funkcionalnosti komponent varnostnega sistema, nadgradnjami in varnostnimi popravki,
- obnovitev podatkov iz varnostnih kopij, zlasti baz podatkov, zadnje delujoče verzije aplikacije, uporabniških datotek,
- zajem nujnih podatkov za namen obravnave incidenta in zavarovanja dokazov, zlasti z zajemom slik zaslona, varnostnim kopiranjem datotek in sistemskih dnevnikov, kopiranjem ali odstranjevanjem in pečatenjem diskov.

Direktor lahko:

- ustanovi skupino za odziv na varnostni incident, ki jo sestavljajo vsaj koordinator informacijske varnosti, vodja področja IT in vodja področja, ki uporablja prizadeti del informacijskega sistema,
- odredi naročilo storitev pogodbenega sistemskega izvajalca,
- odredi delo izven rednega delovnega časa in časa dežurstva ter nadurno delo,
- odredi urgentno naročilo storitev ali opreme,
- odredi druge organizacijske ukrepe.

Spremljanje varnosti in dnevniško beleženje dogodkov

65. člen

Za zagotavljanje ustrezne ravni informacijske varnosti se v agenciji izvaja dnevniško spremljanje sistemskih dogodkov informacijskega sistema. Izvaja se preko sistemov Windows server event, spremljanja alarmov SCOM Microsoft, varnostnega sistema Sophos ali primerljivih orodij.

Sistemski dnevnik dogodkov vsebuje zapise o dogodkih operacijskega sistema in prikazuje informativne dogodke, napake in opozorila. Strežniški dnevniki dogodkov so dnevniške datoteke, ki se samodejno kreirajo in vsebujejo seznam aktivnosti, ki jih strežnik izvaja.

Pri uporabi in hrambi dnevnikov dogodkov, ki vsebujejo osebne podatke, se upoštevajo temeljna načela obdelave osebnih podatkov: zakonitost, poštenost in transparentnost, sorazmernost, točnost in ažurnost, rok hrambe, zavarovanje osebnih podatkov, upoštevanje pravic posameznika.

Ob upoštevanju temeljnih načel se določi roke hrambe dnevnikov dogodkov za posamezne vrste dnevnikov, najdaljši dovoljeni čas hrambe zapisov v dnevnikih s sprotnim dostopom (online) je tri mesece, v varnostnih in arhivskih kopijah pa še dodatnih 12 mesecev.

Dostop do zapisov v sistemskih dnevnikih dogodkov s sprotnim dostopom je varovan in omejen na administratorje sistemov, ki generirajo sistemske dnevnike.

Dostop do zapisov v sistemskih dnevnikih dogodkov v varnostnih in arhivskih kopijah je varovan in omejen na osebe, ki jih pisno pooblasti direktor agencije.

Seznam informacijskih sistemov in njihovih skrbnikov

66. člen

Evidenca aplikacij, vsebinskih skrbnikov aplikacij in informacijskih skrbnikov aplikacij se vodi v elektronski obliki. Evidenco vodi enota za IT, podatki v evidenci so dostopni vsem zaposlenim v agenciji.

Tveganja informacijske varnosti

67. člen

Enota za IT izvaja letne ocene tveganj informacijske varnosti, kar se evidentira v sistemu kakovosti. Pri tem se navede najmanj opise ukrepov, izvajalce in roke izvedbe ukrepov.

Dostop do podatkov

68. člen

Vzpostavljeni morajo biti mehanizmi, ki preprečujejo nepooblaščen dostop do podatkov, ter organizacijski in tehnični postopki, ki preprečujejo nepooblaščeno obdelavo podatkov, vključno s spreminjanjem oziroma uničenjem.

69. člen

Vse evidence dejavnosti obdelav osebnih podatkov (elektronske in papirne) morajo imeti vzpostavljene dnevnike vpogledov, v katerih je zabeleženo kdo in kdaj je opravil vpogled, skladno z veljavno zakonodajo.

Dostop do evidence dejavnosti obdelav osebnih podatkov v elektronski obliki mora biti zaščiten z ustreznimi dostopnimi pravicami (npr. uporabniško ime in geslo, certifikat in geslo, enkratno geslo, fizično varovanje).

70. člen

Vse evidence in dokumenti, ki vsebujejo poslovne skrivnosti, morajo imeti vzpostavljene dnevnike vpogledov, v katerih je zabeleženo kdo in kdaj je opravil vpogled, skladno z veljavno zakonodajo.

Dostop do evidence ali dokumenta, ki vsebuje poslovne skrivnosti, mora biti zaščiten z ustreznimi dostopnimi pravicami (npr. uporabniško ime in geslo, certifikat in geslo, enkratno geslo, fizično varovanje).

71. člen

Dostopne pravice morajo biti urejene tako, da omogočajo posamezniku dostop do najmanjšega možnega nabora podatkov, ki so potrebni za opravljanje nalog.

72. člen

Avtomatsko se beležijo servisni in vzdrževalni posegi na strežniku, bazi, aplikaciji ali storitvi.

73. člen

Uporabniška imena, gesla, kartice za preverjanje dostopa, certifikati in drugi odobreni dostopni mehanizmi ter s tem pridobljene pravice dostopa do sklopov informacijskih sistemov in podatkov so vedno izdani na eno osebo in so neprenosljivi. Posojanje ni dovoljeno.

74. člen

Geslo uporabnika sistema je namenjeno samo njegovi uporabi, zato so uporabniki sistemov odgovorni za vse aktivnosti, ki se zgodijo z uporabo njihove identitete. Gesla se ne smejo zapisovati na papir ali shranjevati na kakršenkoli drug način, ki bi drugi osebi lahko omogočil dostop do gesla. Geslo ne sme vsebovati imena in priimka uporabnika ali njegovih družinskih članov, katerekoli oblike datuma rojstva, imena, oznake ali številke agencije ter zaporednih števil.

Pri izbiri in menjavi gesel so uporabniki dolžni upoštevati naslednja pravila:

- izbirati je treba gesla z najmanj osmimi znaki,
- geslo je sestavljeno iz najmanj treh različnih znakov, od katerih je vsaj ena črka ali simbol,
- gesla ne vsebujejo šumnikov,
- gesla je treba menjati vsaj enkrat vsakih šest mesecev,
- vsaj pet zaporednih gesel je neponovljivih.

75. člen

Prostori, v katerih se obravnavajo podatki, morajo biti varovani z organizacijskimi, fizičnimi in tehničnimi ukrepi, ki nepooblaščenim osebam onemogočajo dostop do podatkov in sredstev informacijske tehnologije, s katero se slednji obdelujejo.

Pri elektronskih evidencah podatkov morajo biti izpolnjeni organizacijsko-tehnični pogoji za vzdrževanje teh evidenc ter zagotovljeni postopki za varnostno shranjevanje in arhiviranje teh podatkov, skladno z veljavno zakonodajo.

76. člen

Zaposleni morajo varovati zaupne podatke, s katerimi so se seznanili med trajanjem delovnega razmerja. Varovati jih morajo tudi po prenehanju delovnega razmerja.

Nabava informacijske opreme

Priprava naročila

77. člen

Pri pripravi specifikacij naročila za nabavo gradnikov ali vzdrževanje sklopov informacijskih sistemov je treba predvideti in opredeliti varnostne elemente, ki bodo izpolnjevali zahteve IVP in veljavne zakonodaje.

Varnostni elementi v pogodbah

78. člen

V pogodbah morajo biti določeni predmet in obseg storitve, merila, obveznosti in s tem povezane posledice, ki vplivajo na kakovostno izvedbo pogodbenih obveznosti glede IVP.

Pogodbe z zunanjimi izvajalci morajo vsebovati določbo o seznanjenosti z IVP in sprejemanju te politike ter zavezanost k varovanju podatkov, kjer je to potrebno.

Zunanji izvajalci in podizvajalci, ki bodo izvajali dela po pogodbi, morajo pred sklenitvijo pogodbe podpisati izjave o seznanitvi z IVP in sprejemanju te politike.

Za veljavne pogodbe, sklenjene pred uveljavitvijo IVP, je treba z izvajalci skleniti dodatke k pogodbam in podpisati izjave, kjer je to smiselno in izvedljivo.

79. člen

V pogodbah, po katerih zunanji izvajalci obdelujejo podatke, mora biti natančno opredeljeno, katere podatke obdelujejo, kako se lahko obdelujejo ter kdo jih lahko obdeluje.

80. člen

Dostopi in posegi zunanjih izvajalcev v informacijske sisteme agencije morajo biti beleženi v informacijskem sistemu.

81. člen

Za omrežje in njegovo varnost je na agenciji zadolžena enota za IT. Ta stalno preverja integriteto omrežja.

82. člen

Upravljanje informacijskega sistema in omrežij mora biti razdeljeno na več nalog, ki jih, če je to mogoče, opravljajo različne osebe. Izvajanje nalog je treba nadzorovati.

ODGOVORNOST ZA KRŠITEV DOLOČB

83. člen

Kršitev določb tega pravilnika s strani zaposlenih v agenciji pomeni kršenje obveznosti iz delovnega razmerja, ostali pa za kršitve odgovarjajo na temelju pogodbenih obveznosti.

Odgovornost iz prejšnjega odstavka ne izključuje kazenske ali odškodninske odgovornosti, skladno z veljavno zakonodajo.

KONČNA DOLOČBA

84. člen

Ta pravilnik začne veljati naslednji dan po sprejemu in se objavi na intranetnih straneh agencije, obvestilo o objavi pa se po elektronski pošti posreduje vsem zaposlenim v agenciji.

Številka: 05-2/2021-1
Datum: 18.11.2021

Franjo Levstik
predsednik Sveta JAZMP