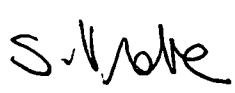
PRAVILNIK O POSTOPKIH IN UKREPIH PRI DELOVANJU IN VZDRŽEVANJU INFORMACIJSKEGA OKOLJA INFORMACIJSKEGA POOBLAŠČENCA

Verzija dokumenta:	1.5
Datum veljavnosti:	6. 5. 2019
Skrbnik dokumenta:	namestnik - delovno področje informacijske tehnologije
Oznaka dokumenta:	020-5/2010/84

Zgodovina dokumenta

Verzija dokumenta	Status	Bistvene spremembe glede na prejšnjo verzijo	Datum začetka veljave
1.0	končna	obravnavani predlogi zunanjega svetovalca in Arhiva RS	5. 5. 2011
1.1	dopolnjena	ureditev postopka kriptiranja podatkovnih nosilcev v delovnih postajah	14.11.2011
1.2	dopolnjena	prilagoditev določb glede na spremenjeno dejansko stanje po selitvi IP na novo lokacijo (15.3.2013), nove določbe glede BYOD	5.4.2013
1.3	dopolnjena	dodane določbe glede hrambe predalov elektronske pošte po prekinitvi zaposlitve in hrambe/brisanja podatkov na mrežnih pogonih	19.10.2015
1.4	dopolnjena	Dodane določbe o uporabi wifi omrežja	20. 11. 2017
1.5	dopolnjena	Spremembe zaradi uveljavitve Splošne uredbe o varstvu podatkov in selitve na novo lokacijo	6. 5. 2019

Priprava, pregled in potrditev

Podpisnik in funkcija podpisnika	Datum podpisa	Podpis
mag. Andrej Tomšič, namestnik IP		
mag. Sanja Vraber, generalna sekretarka		
Mojca Prelesnik, informacijska pooblaščenka		

Na podlagi 24. in 25. člena Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo; v nadaljevanju: ZVOP-1), 32. člena Splošne uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba)) in 3. odstavka 2. člena Zakona o Informacijskem pooblaščencu (Uradni list RS, št. 113/05 in 51/07 – ZUstS-A, ZInfP) izdaja Informacijski pooblaščenec naslednji

PRAVILNIK

o postopkih in ukrepih pri delovanju in vzdrževanju informacijskega okolja Informacijskega pooblaščenca

I. SPLOŠNE DOLOČBE

Vsebina in namen pravilnika

1. člen

(1) S tem pravilnikom se določajo organizacijski, tehnični in logično-tehnični postopki in ukrepi glede delovanja in vzdrževanja informacijskega sistema in informacijske opreme Informacijskega pooblaščenca (v nadaljevanju IP).

(2) Zaposleni pri IP morajo biti seznanjeni z vsebino tega pravilnika.

Pomen izrazov

2. člen

V tem pravilniku uporabljeni izrazi imajo naslednji pomen:

1. Informacijsko okolje IP – sestoji iz programske in strojne opreme; strojna oprema vključuje strežnike, aktivno in pasivno omrežno opremo, lokalne delovne postaje s pripadajočimi perifernimi napravami, tiskalnike in fotokopirne naprave, enote za varnostno kopiranje, prenosne nosilce podatkov in drugo strojno opremo, ki je v lasti Informacijskega pooblaščenca.
2. Lokalna delovna postaja – je namizni ali prenosni osebni računalnik, ki je dan v uporabo zaposlenemu.
3. Zasebni mrežni pogon – je mrežno mesto na strežniku IP za shranjevanje podatkov, do katerega ima dostop samo vsak posamezni zaposleni (oznaka: I:/).
4. Skupni mrežni pogon – je mrežno mesto na strežniku IP za shranjevanje skupnih podatkov (oznaka: J:/) in je dostopno vsem zaposlenim z izjemo posameznih imenikov na tem mestu, kot je prekrškovna evidenca, do katere imajo dostop samo pooblaščene osebe.
5. Nosilec podatkov - so vse vrste sredstev, na katerih so zapisani ali posneti podatki (listine, akti, gradiva, spisi, računalniška oprema vključno z magnetnimi, optičnimi ali drugimi računalniškimi mediji, fotokopije, zvočno in slikovno gradivo, mikrofilmi, naprave za prenos podatkov, ipd.).
6. Intranet IP – je spletno mesto za interno komuniciranje med zaposlenimi pri Informacijskem pooblaščencu. Nahaja se na naslovu: http://panacea/intranet. Na intranetu se med drugim objavljajo pravilniki in navodila, ki jih sprejema Informacijski pooblaščenec.
7. Orodje za podporo na daljavo – je programska oprema, ki omogoča dostop in upravljanje z lokalno delovno postajo na daljavo; med to opremo sodi zlasti Remote Desktop Connection in VNC (Virtual Network Computing).

II. VAROVANJE OPREME, PROSTOROV IN KOMUNIKACIJSKE INFRASTRUKTURE

3. člen

(1) Dostop do sistemskih sob je dovoljen osebam, ki so odgovorne za delovanje informacijskega sistema IP (Delovno področje informacijske tehnologije), informacijski pooblaščenki ter drugim zaposlenim pri IP, ki imajo za to pisno pooblastilo informacijske pooblaščenke. Dostop do sistemskih sob je mogoč s ključem ali elektronsko kartico, ki je dodeljena pooblaščenim osebam.

(2) Osebe, ki niso zaposlene pri IP (npr. vzdrževalci prostorov, strojne in programske opreme, obiskovalci, poslovni partnerji) smejo vstopiti v sistemske sobe v prisotnosti vsaj ene od oseb iz 1. odstavka tega člena razen v izrednih primerih (varnostna služba v primeru suma vloma, požara).

(3) Vsak vstop v sistemske sobe se mora zabeležiti. Zabeleži se datum vstopa in enolična identifikacija osebe, ki je vstopila. Vstopi v sistemske sobe se beležijo v elektronsko vodeni evidenci vstopov z elektronsko kartico, ki beleži številko kartice, datum in čas vstopa. Evidenco vstopov v sistemsko sobo se redno pregleduje (najmanj enkrat letno) s strani oseb, ki so odgovorne za delovanje informacijskega sistema IP.

(4) Vpogled v arhiv posnetkov videonadzornega sistema opravi tričlanska komisija, ki jo s pisnim sklepom imenuje informacijska pooblaščenka. Vpogled v arhiv posnetkov videonadzornega sistema se beleži v za to namenjeno evidenco na papirnem obrazcu, ki se nahaja v sistemski sobi. Pri vsakem vpogledu se zabeleži ime in priimek, datum in namen vpogleda, podatke o posnetkih ter podatke o iznosu posnetkov, če so se iznašali.

(5) Sistemske sobe se varujejo z varnostnimi ukrepi in postopki za zaščito pred okoljskimi nevarnostmi, in sicer s klimatskimi napravami za zagotavljanje ustreznega temperaturnega območja, sistemom za proženje alarmov, ki je povezan z operativnim centrom Sintal in sistemom UPS za neprekinjeno napajanje. Računalniška oprema (strežniki, diskovna polja, delovne postaje in druga oprema) mora biti nameščena v pogojih, ki so skladni s tehničnimi specifikacijami opreme. Ustreznost delovanja varnostnih naprav preverjajo osebe, ki so odgovorne za delovanje informacijskega sistema na tedenski ravni, o tem se vodijo pisni zapisi. Vsi varnostni ukrepi in naprave morajo delovati v vsakem trenutku (tudi izven delovnega časa).

(6) Električna in telekomunikacijska napeljava mora biti izvedena tako, da je ni možno nenamerno prekiniti ali brez večjih težav uničiti ali zlorabiti.

(7) V primeru razvoja ali testiranja informacijskih rešitev morata biti razvojno in testno okolje medsebojno ločena ter ločena od operativnega okolja. Če se pri testiranju ali razvoju uporablja podatke iz operativnega okolja, je z njimi potrebno ravnati na enak način, kot s podatki iz operativnega okolja, podatke v razvojnem in testnem okolju pa po uporabi ustrezno uničiti.

(8) Dostop do podatkov preko aplikativne programske opreme se varuje s sistemom gesel za avtentikacijo in avtorizacijo uporabnikov. Sistem gesel mora omogočati tudi možnost naknadnega ugotavljanja, kdaj je bil opravljen posamezen dostop do posameznega informacijskega podsistema, kdo ga je izvedel in do katerih podatkov je dostopal (revizijske sledi). Ustreznost zapisovanja revizijske sledi se redno pregleduje s strani oseb, ki so odgovorne za delovanje informacijskega sistema IP.

(10) Usklajenost sistemskih ur znotraj informacijskega okolja IP se redno preverja. Uskladitev sistemskih ur v odnosu do zunanjih izvajalcev poteka na podlagi predhodnega dogovora z zunanjim izvajalcem. Ura videonadzornega sistema se ročno usklajuje z uro protivlomnega sistema.

III. UPORABA INFORMACIJSKO-KOMUNIKACIJSKIH TEHNOLOGIJ

Prihod na novo zaposlenega ter prevzem opreme

4. člen

(1) Osebe, ki so odgovorne za delovanje informacijskega sistema IP, zaposlenemu ob sklenitvi delovnega razmerja pripravijo in predajo lokalno delovno postajo.

(2) Vsem zaposlenim na IP se zagotovi dostop do skupnih datotek (skupni mrežni pogon), možnost shranjevanja datotek, do katerih ima dostop samo posamezen zaposleni (zasebni mrežni pogon) ter dostop do elektronske pošte in zadev v SPIS aplikaciji, ki so signirane na zaposleno osebo.

Upravljanje uporabniških pravic

5. člen

(1) Vsakemu uporabniku se dodeli unikatno uporabniško ime, ki ga lahko uporablja samo lastnik. Zahtevek za dodelitev uporabniškega imena in upravljanje uporabniških pravic je dosegljiv na intranetu (*Obrazec za upravljanje uporabniških pooblastil*). Ob prihodu novozaposlenega ga predlagatelj zahtevka (kadrovska služba) v izvedbo po elektronski pošti posreduje informatiku. Informatik v primeru potrebe po spremembi uporabniških pravic zaradi premestitve, spremembe obsega delovnih nalog ali iz drugih utemeljenih razlogov, na podlagi zahtevka s strani posamezniku neposredno nadrejenih oseb ali informacijske pooblaščenke, izvede ustrezno spremembo uporabniških pravic (sprememba, odvzem, dodelitev).

(2) Posojanje uporabniškega imena ni dovoljeno. Prav tako ni dovoljena uporaba skupinskih uporabniških imen.

(3) Zaposleni na svojih delovnih postajah ne smejo imeti administratorskih pravic. Administratorske pravice imajo na svojih delovnih postajah le informacijska pooblaščenka in osebe, ki so odgovorne za delovanje informacijskega sistema IP.

(4) Uporabniške pravice morajo biti skladne z nalogami in deli, ki jih opravlja posamezni zaposleni.

(5) V primeru potrebe po namestitvi dodatne programske ali strojne opreme, se zaposleni obrne na osebe, ki so odgovorne za delovanje informacijskega sistema IP.

(6) Izjemoma se lahko na predlog informacijske pooblaščenke posameznim uporabnikom zaradi narave njihovega dela dodeli oziroma odvzame pravice lokalnega administratorja delovne postaje, ki tem uporabnikom omogočajo namestitev dodatne programske opreme na delovnih postajah, ki jih uporabljajo.

(7) Zaposleni ne smejo nameščati programske ali strojne opreme brez vednosti oseb, ki so odgovorne za delovanje informacijskega sistema IP, razen če so podani pogoji iz prejšnjega odstavka.

(8) V primeru sporov glede nameščanja programske opreme na željo zaposlenega ali odkritja zlonamerne programske opreme so osebe, odgovorne za delovanje informacijskega sistema IP, dolžne obvestiti informacijsko pooblaščenko.

(9) Pravico vnašanja, brisanja in upravljanja z dokumenti v elektronskem dokumentnem sistemu (SPIS) imajo samo osebe v Administrativno tehnični službi. Uporabniki na delovnih področjih Delovno področje informacij javnega značaja in Delovno področje varstva osebnih podatkov imajo v okolju Lotus Notes dostop samo do svojih zadev in podatkov. Dostop do gradiva v sistemu za dolgoročno hrambo dokumentarnega gradiva pri zunanjem izvajalcu je možen samo iz elektronskega dokumentnega sistema (SPIS) osebe v Administrativno tehnični službi ob zagotavljanju beleženja dostopov. Upravljanje dostopnih pravic zaposlenih v Administrativno tehnični službi poteka skladno z ostalimi določbami tega pravilnika in Pravilnika o postopkih in ukrepih za varnost osebnih podatkov.

Podpora uporabnikom

6. člen

(1) Osebe, ki so odgovorne za delovanje informacijskega sistema IP, dajejo uporabnikom podporo pri delovanju in vzdrževanju strojne in programske opreme.

(2) Zahtevek za poseg glede delovanja strojne ali programske opreme se poda ustno ali pisno na služben elektronski naslov informatika.

(3) Zahtevek se pregleda in izvede v roku, ki je primeren glede na nujnost, obseg in težavnost zahtevka.

(4) Podpora na daljavo z uporabo orodij, kot so Remote Desktop Connection za administratorska dela ali VNC, ki deluje samo v lokalni mreži preko kriptirane povezave za podporo uporabnikom, se lahko uporabljajo samo z vnaprejšnjo privolitvijo zaposlenega.

Uporaba interneta in elektronske pošte

7. člen

(1) Glede uporabe interneta in elektronske pošte se uporabljajo določbe Pravilnika o postopkih in ukrepih za varnost osebnih podatkov, ki je objavljen na intranetu IP.

(2) Na predlog informacijske pooblaščenke se zaposlenemu lahko omogoči oddaljen dostop do lastne službene elektronske pošte preko VPN povezave in z uporabo geselnika za varni dostop.

Varnostno kopiranje in posodabljanje varnostnih mehanizmov

8. člen

(1) Osebe, ki so odgovorne za delovanje informacijskega sistema IP, so zadolžene za varnostno kopiranje podatkov v informacijskem sistemu IP.

(2) Za potrebe restavriranja informacijskega sistema ob okvarah in ob drugih izjemnih situacijah se vsak delovni dan zagotavlja redna izdelava varnostnih kopij vseh produkcijskih strežnikov.

(3) Rezervna varnostna kopija se izvaja enkrat mesečno na kriptirani trdi disk. Trdi disk se ne sme nahajati v isti sobi kot strežniki.

(4) Podatke, ki izvirajo iz delovnega procesa zaposlenih, si zaposleni shranjujejo ali kopirajo na zasebnih mrežnih pogonih - Private\ (I:), ki se dnevno varnostno kopirajo. Za morebitno izgubo podatkov na lokalnih diskih ob okvarah in ob drugih izjemnih situacijah odgovarja vsak zaposleni sam. Arhivske poštne baze se shranjujejo na zasebni mrežni disk ali na disk lokalne delovne postaje.

(5) Skupni mrežni pogon se dnevno varnostno kopira. V izogib težavam pri preglednosti in uporabnosti skupnega mrežnega pogona ter nesorazmernim obremenitvam za sistem varnostnega kopiranja, se morajo zaposleni izogibati shranjevanju datotek na skupni mrežni pogon, ki tja ne spodijo, kot so fotografije in zaslonske slike z inšpekcijskih ogledov, dokumenti iz konkretnih inšpekcijskih postopkov, dokumenti, slike ali video posnetki zasebne narave, zbirke varovanih osebnih podatkov. V ta namen morajo zaposleni periodično brisati neprimerne datoteke s skupnega mrežnega pogona. Informatik enkrat letno s skupnega mrežnega pogona pobriše vsebine, ki po določbah tega pravilnika ne sodijo na skupni mrežni pogon. Informatik to stori do 31.1. za preteklo leto.

(6) Pri zagotavljanju shranjevanja podatkov iz prejšnjega odstavka nudijo zaposlenim pomoč osebe, ki so odgovorne za delovanje informacijskega sistema IP.

(7) Osebe, ki so odgovorne za delovanje informacijskega sistema IP, so zadolžene za redno nameščanje varnostnih popravkov ter posodabljanje protivirusne zaščite.

(8) Informacijska infrastruktura mora biti zaščitena proti virusi, škodljivo ter nezaželeno programsko kodo in vsebino. Vsebina diskov mrežnega strežnika in lokalnih delovnih postaj, kjer se nahajajo osebni podatki, se vsakodnevno preveri z vidika prisotnosti računalniških virusov. Ob pojavu računalniškega virusa se tega čim prej odpravi, obenem pa se ugotovi vzrok pojava virusa v informacijskem okolju Informacijskega pooblaščenca. Vsi podatki in programska oprema, ki so namenjeni uporabi v informacijskem okolju Informacijskega pooblaščenca, in prispejo k Informacijskemu pooblaščencu na medijih za prenos računalniških podatkov ali preko komunikacijskih kanalov, morajo biti pred uporabo preverjeni z vidika prisotnosti računalniških virusov. Uporabniki lahko osebe, ki so odgovorne za delovanje informacijskega sistema prosijo, da preverijo prisotnost virusov, škodljive ter nezaželene programske kode in vsebine na opremi uporabnika. V tem primeru se preverjanje opravi na ločeni delovni postaji, ki ni priključena v omrežje. Protivirusni program, operacijski sistemi in programska oprema se redno posodabljajo, prav tako se s posebno programsko opremo nadzira nameščene popravke in nadgradnje.

Režim izbire, dodeljevanja, hranjenja in spreminjanja gesel

9. člen

(1) Zaposleni morajo uporabljati gesla, ki so sestavljena iz kombinacije najmanj 8 črk, številk in posebnih znakov. Geslo ne sme vsebovati besed, ki jih lahko najdemo tudi v slovarjih, pojmov, ki imajo posebno povezavo s posameznikom (kot so npr. posameznikovo ali partnerjevo ime, ime hišnega ljubljenčka, rojstni datumi in podobno) ter delov ali celote uporabniškega imena.

(2) Zahteve iz prejšnjega odstavka veljajo tudi za gesla, ki se uporabljajo za zagon kriptiranih delovnih postaj, le da mora biti takšno geslo sestavljeno iz najmanj 8 črk, številk in posebnih znakov.

(3) Gesli za vstop v operacijski sistem delovne postaje in okolje Lotus Notes se morata razlikovati.

(4) Osebe, ki so odgovorne za delovanje informacijskega sistema IP, dajejo zaposlenim pomoč pri izbiri in spreminjanju gesel.

(5) Gesla za vstop v operacijski sistem delovne postaje se spreminjajo najmanj vsake tri mesece. Sistem aktivnega direktorija uporabnike avtomatsko opozarja na potek veljavnosti obstoječega gesla in potrebo po zamenjavi gesla. Starih gesel ni dovoljeno ponovno uporabljati.

(6) Sistemska gesla so shranjena v kriptirani datoteki, ki je shranjena na mrežnem disku. Dostop do datoteke imajo samo osebe, ki so odgovorne za delovanje informacijskega sistema IP ter informacijska pooblaščenka. Vsak dostop do datoteke s sistemskimi gesli se zabeleži.

(7) Gesla za zagon kriptiranih delovnih postaj se hranijo v kriptirani datoteki, obnovitveni CD-ji (rescue disk) se hranijo na varnem mestu pod nadzorom oseb, ki so odgovorne za delovanje informacijskega okolja IP. Gesla za zagon kriptiranih delovnih postaj omogočajo samo zagon operacijskega sistema in ne omogočajo dostopa do podatkov uporabnika.

(8) Zaposleni morajo delovne postaje ob izhodih iz pisarne zaradi preprečitve dostopa nepooblaščenih oseb zakleniti (politika čistega zaslona) s pomočjo tipk WIN+L. Osebe, ki so odgovorne za delovanje informacijskega sistema IP, na delovnih postajah namestijo samodejno zaklepanje zaslona po 10 minutah neaktivnosti. Vstop v računalnik po zaklepanju je možen samo z vnosom gesla.

(9) Ob koncu delovnega dne morajo zaposleni fizično ugasniti svoje delovne postaje.

Varnost podatkov na delovnih postajah

10. člen

(1) Dostop do posameznikovega uporabniškega profila na operacijskem sistemu je zavarovan z ustreznim sistemskim geslom.

(2) Podatkovni nosilci v namiznih in prenosnih delovnih postajah se v celoti kriptirajo na način, ki onemogoča seznanitev z vsebino shranjenih podatkov brez vnosa ustreznega gesla. Pred izvedbo kriptiranja podatkovnih nosilcev delovnih postaj se pripravi obnovitveno datoteko, ki omogoča odpravo napak pri zagonu podatkovnih nosilcev.

(3) Na delovnih postajah se ne smejo nahajati zaupni podatki v nekriptirani obliki. Podatki, ki niso potrebni za opravljanje delovnih nalog izven IP, se hranijo na mrežnih pogonih in ne na prenosnikih.

(4) Delovne postaje se izven delovnega mesta ne sme puščati izven nadzora ali dajati v uporabo tretjim osebam brez vednosti zaposlenega.

(5) Pri zagotavljanju varnosti podatkov na delovnih postajah nudijo zaposlenim pomoč osebe, ki so odgovorne za delovanje informacijskega sistema IP.

(6) Zaposleni, ki prenosne delovne postaje izven delovnega časa puščajo v pisarni, imajo na voljo varnostni kabel za zaklepanje prenosnika.

Varnost prenosnih nosilcev podatkov

11. člen

(1) Zaposleni, katerim so bili dodeljeni prenosni nosilci podatkov (USB ključi, prenosni diski in ostali prenosni nosilci podatkov), so odgovorni za varnost teh nosilcev.

(2) Prenosni nosilci podatkov v postopkih inšpekcijskega ogleda ne smejo vsebovati podatkov iz drugih inšpekcijskih, prekrškovnih ali drugih službenih ali zasebnih zadev.

(3) Po uporabi prenosnih nosilcev podatkov se vsebina teh nosilcev shrani v okviru informacijskega sistema IP ali izbriše.

(4) O morebitni izgubi ali kraji prenosnih nosilcev podatkov, mora zaposleni takoj obvestiti osebe, ki so odgovorne za delovanje informacijskega sistema IP. O izgubi se sestavi uradni zaznamek, v katerem se navede okoliščine ter popiše vsebina podatkov na izgubljenih prenosnih nosilcih podatkov.

Postopanje ob prekinitvi delovnega razmerja

12. člen

(1) Ob prekinitvi delovnega razmerja se zaposlenemu ukinejo vse dostopne pravice v informacijskem okolju IP in se ob temu ustrezno izpolni Obrazec za upravljanje uporabniških pooblastil.

(2) Zaposlenemu mora biti dana možnost, da lahko pred prekinitvijo delovnega razmerja s službenih sredstev, ki so mu bila dodeljene v uporabo, pobriše ali si skopira osebne podatke in zasebno korespondenco, ki je nastala ob uporabi službenih sredstev v izključno zasebne namene.

(3) Ob prekinitvi delovnega razmerja zaposleni in oseba, ki je odgovorna za delovanje informacijskega sistema IP, podpišeta primopredajni zapisnik, v katerem popišeta delovna sredstva, ki jih zaposleni vrača. Sestavni del primopredajnega zapisnika je tudi izjava zaposlenega, s katero ta izjavlja:

a) da mu je bila dana možnost zavarovanja lastnih osebnih podatkov in zasebne korespondence, ki je nastala ob uporabi službenih sredstev v izključno zasebne namene,
b) da delovna sredstva, ki jih vrača delodajalcu, ne vsebujejo njegovih osebnih podatkov ali osebne korespondence in da se lahko morebitni neizbrisani osebni podatki in osebna korespondenca na vrnjenih delovnih sredstvih nepovratno uničijo z naključnim prepisovanjem in formatiranjem.

(4) Predal elektronske pošte zaposlenega, ki mu je prenehalo delovno razmerje pri IP, se na poštnem strežniku hrani 1 leto od prekinitve delovnega razmerja nato se izbriše.

Uničenje in odpis informacijskih sredstev

13. člen

(1) Ustreznost delovanja informacijskih sredstev v okviru Informacijskega okolja IP redno preverja informatik in o ugotovitvah poroča vodji Delovnega področja informacijske tehnologije.

(2) UNIČENJE: v primeru, da je potrebno določeno informacijsko sredstvo ali opremo zaradi izrabljenosti, okvare, tehnološkega zastaranja ali iz drugih utemeljenih razlogov odpisati oziroma uničiti, mora informatik v sodelovanju s Administrativno tehnično službo IP ali komisija, imenovana s sklepom informacijske pooblaščenke, pripraviti predlog za uničenje opreme ob upoštevanju predpisov, ki opredeljujejo ravnanje z odsluženo opremo. Predlog mora odobriti informacijska pooblaščenka. Pred uničenjem nosilcev podatkov informatik poskrbi, da je vsebina nosilcev podatkov nepovratno izbrisana.

(3) Na podlagi odobrenega predloga o uničenju informatik informacijsko sredstvo ali opremo preda v komisijsko uničenje, ki mora potekati v prisotnosti informatika. Po uničenju informatik pridobi potrdilo o uničenju, katerega preda Administrativno tehnični službi IP, ki izvede postopek odpisa informacijskega sredstva.

(4) Uničevanje drugih informacijskih virov, kot je dokumentarno gradivo, poteka skladno z veljavnimi določbami Uredbe o upravnem poslovanju.

(5) ODPIS: informacijskih sredstev poteka skladno z določbami zakonodaje, ki opredeljuje postopke upravljanja s premoženjem države.

(6) V primeru odtujitve informacijskega sredstva (kraja, izguba), Administrativno tehnična služba IP pridobi izjavo zaposlenega, policijski zapisnik ali drugo ustrezno dokazilo o odtujitvi informacijskega sredstva.

(7) Odpis informacijskih sredstev se izvede na podlagi predloga o odpisu, ki ga pripravi informatik v sodelovanju s Administrativno tehnično službo IP ali komisija, imenovana s sklepom informacijske pooblaščenke. Predlog mora odobriti informacijska pooblaščenka.

(8) Na podlagi odobrenega predloga o odpisu Administrativno tehnična služba IP na Ministrstvo za finance pošlje vso potrebno dokumentacijo za odpis osnovnega sredstva iz registra osnovnih sredstev.

Uporaba zasebnih sredstev v Informacijskem okolju IP (Bring-YourOwn-Device; BYOD)

14. člen

(1) Uporaba zasebnih informacijsko-komunikacijskih sredstev, kot so prenosni računalniki, tablice, pametni telefoni, prenosni mediji in drugih zasebnih sredstev v Informacijskem okolju IP, je dovoljena, če je to potrebno zaradi opravljanja delovnih nalog in na podlagi predhodnega pisnega dovoljenja informacijske pooblaščenke.

(2) Namestitev programske opreme za dostop do Informacijskega okolja IP in dodelitev, sprememba ali odvzem pripadajočih uporabniških pravic na zasebna informacijsko-komunikacijska sredstva je možna samo na podlagi predhodnega pisnega dovoljenja informacijske pooblaščenke.

(3) Zasebna informacijsko-komunikacijskih sredstva mora biti pred uporabo in med uporabo preverjena glede prisotnosti virusov, škodljive ter nezaželene programske kode in vsebine. Zaposleni mora osebam, ki so odgovorne za delovanje informacijskega okolja IP, izkazati prisotnost ustreznih varnostnih kontrol na svoji napravi (protivirusna zaščita ipd.).

(4) V primeru sporov glede uporabe zasebnih sredstev v Informacijskem okolju IP so odgovorne osebe za delovanje informacijskega sistema IP dolžne obvestiti informacijsko pooblaščenko.

(5) Zasebnih informacijsko-komunikacijskih sredstev se ne sme vključevati v domeno IP.

Brezžično omrežje IP (IPRS Gost)
14.a

(1) IP omogoča zaposlenim in obiskovalcem dostop do prostega interneta preko brezžične dostopne točke (SSID oznaka: IPRS Gost). Dostop je mogoč z vnosom gesla, ki je objavljeno na intranetu. Obiskovalcem se lahko na njihovo prošnjo razkrije geslo za dostop do brezžične točke IP.

(2) Prosti internet ni del omrežja HKOM, zato prek brezžične dostopne točke IP brez dodatnega povezovanja v VPN HKOM ni mogoče dostopati do podatkov na strežnikih IP (kar vključuje tudi mrežne pogone in službene predale elektronske pošte).

(3) Uporaba brezžičnega omrežja IP je namenjena izvajanju delovnih nalog zaposlenih, ki jih zaradi omejitev v HKOM omrežju sicer ne bi bilo mogoče izvesti ter uporabi s strani obiskovalcev.

(4) IP lahko kadarkoli omeji ali onemogoči dostop do svojega brezžičnega omrežja.

IV. ODGOVORNOST ZA IZVAJANJE POSTOPKOV IN UKREPOV ZA NEMOTENO IN VARNO DELOVANJE INFORMACIJSKEGA OKOLJA INFORMACIJSKEGA POOBLAŠČENCA

Odgovornost za kršitev

15. člen

(1) Kršitev določil tega pravilnika s strani zaposlenih pomeni kršenje obveznosti iz delovnega razmerja.

(2) Odgovornost iz prejšnjega odstavka ne izključuje kazenske ali odškodninske odgovornosti.

V. KONČNE DOLOČBE

Začetek veljavnosti

16. člen

Ta pravilnik prične veljati naslednji dan po objavi na intranetu IP.

17. člen

Z dnem začetka veljave tega pravilnika preneha veljati Pravilnik o postopkih in ukrepih pri delovanju in vzdrževanju informacijskega okolja Informacijskega pooblaščenca, z dne 20. 11. 2017, številka 020-5/2010/79.

Informacijski pooblaščenec:
Mojca Prelesnik, univ. dipl., prav.,
pooblaščenka

Datum: 6. 5. 2019