Na temelju članka 20. i 45. Statuta Instituta za poljoprivredu i turizam, a sukladno Odluci o prihvatljivom korištenju CARNET mreže od 15. lipnja 2012. godine, članku 29. Zakona o radu (NN br. 93/14, 127/17), Upravno vijeće je na sjednici održanoj 24. rujna 2018. godine donijelo

P R A V I L N I K
o korištenju računalnog sustava i drugih sredstava komunikacije

Članak 1.

Ovim Pravilnikom uređuje se način korištenja računalne opreme (u daljnjem tekstu: IT oprema) i sustava te elektroničke pošte, mobitela, službenih telefona i drugih oblika komunikacije Instituta za poljoprivredu i turizam (dalje u tekstu: Institut), prava i ovlasti Instituta te prava i obveze korisnika u vezi korištenja opreme i sredstava komunikacije.

Računalna oprema i sustav

Članak 2.

Prihvatljivo korištenje računalnih resursa obvezuje sve zaposlenike i ostale korisnike koji imaju pristup IT sustavu Instituta.

Članak 3.

Sva IT oprema koju je kupio Institut, njegovo je vlasništvo i koristi se u službene svrhe.
Za potrebe posla radnici Instituta dobivaju korisnički račun koji se sastoji od korisničkog imena (username) oblika ime@iptpo.hr i lozinke (password) te dobivaju elektroničku adresu.
Korisnički računi se vode u sklopu AAI@EDU.hr imeničkog sustava.
Korisnički račun, ime i prezime radnika i elektronička adresa pohranjuju se u elektronički imenik Microsoft Active Directory.
Elektronički imenik pohranjen je i zaštićen Microsoftovom tehnologijom prema pravilima struke.
Eventualno „curenje“ odnosno kompromitiranje elektroničkog imenika prijavljuje se CARNET CERT-u i AZOP-u.
Voditelj obrade elektroničkog imenika je Institut (sistem inženjer).

Članak 4.

Za potrebe otvaranja korisničkog računa prikupljaju se sljedeći osobni podaci: ime i prezime. OIB, elektronička adresa, mjesto rada, temeljna povezanost s Institutom (zaposlenik, gost i sl.) te datum isteka temeljne povezanosti.
Minimalna dužina lozinke mora biti osam znakova, sastavljena od mješavine malih i velikih slova, brojeva i drugih znakova.
Korisnici su odgovorni za čuvanje tajnosti svoje lozinke i ni u kom je slučaju ne smiju otkriti niti ostaviti na mjestu dostupnom drugim osobama.
Pri prestanku radnog odnosa sistem inženjer mora osigurati zatvaranje korisničkog računa čime se korisnički račun briše kao i svi pripadni osobni podaci. Iznimno, ravnatelj može odobriti korištenje korisničkog računa i pripadne elektroničke adrese i nakon prestanka radnog odnosa, na određeno ili neodređeno vrijeme.

Članak 5.

Korisnici su dužni služiti se računalima i sustavom poštujući zakone, propise i etičke norme RH i međunarodne.

Institut zadržava pravo nadzora nad načinom korištenja IT opreme i sustava, sukladno zakonu, međunarodnim propisima i aktima Instituta.

Članak 6.

Podaci koji se nalaze na računalnim sustavima pripadaju Institutu ili subjektima koji su od Instituta naručili obavljanje određenih poslova.
Institut dozvoljava korištenje IT sustava za učenje i samorazvoj, napredovanje u struci, pod uvjetom da korisnici preuzimaju punu osobnu odgovornost za svoje aktivnosti, da one ne ometaju obavljanje posla i da se ne narušavaju ostala pravila prihvatljivog korištenja.

Članak 7.

Nije dozvoljeno:
- korištenje nelicenciranog softvera,
- neovlašteno kopiranje medija sa softverom ili drugim materijalom koji podliježe zaštiti autorskog prava ili prava intelektualnog vlasništva,
- preuzimanje tuđeg identiteta (npr. korištenje tuđeg korisničkog imena, slanje pošte pod tuđim imenom, kupovanje preko interneta s tuđom kreditnom karticom itd.)
- ustupanje lozinke ili korisničkog imena drugima.

Korisnik snosi osobnu odgovornost ukoliko krši odredbe prethodnog stavka.
Korisnik je odgovoran za sve što je učinjeno s njegovim identitetom.

Elektronička pošta

Članak 8.

Svaka e-mail adresa koju je otvorio Institut, bez obzira odnosi li se na ustanovu u cjelini ili na pojedinog korisnika, koristi se za rad u Institutu te se smatra službenom e-mail adresom Instituta i u njegovom je vlasništvu (službeni e-mail).

Članak 9.

Pri zapošljavanju novog radnika Institut mu dodjeljuje elektroničku adresu oblika ime(ili kombinacija imena i prezimena)@iptpo.hr.
Poslovne elektroničke adrese radnika javno se objavljuju na mrežnim stranicama http://iptpo.hr.
Elektronička adresa sastavni je dio osobnih podataka zapisanih u elektronički imenik Instituta.
Otvaranje elektroničke adrese u ime Instituta kao voditelja obrade elektroničkog imenika, vrši sistem inženjer.
Za vrijeme trajanja pretplatničkog odnosa, elektronički sandučići radnika pohranjeni su na vlastitoj infrastrukturi.
Elektronička adresa svi@iptpo.hr namijenjena je za slanje važnih informacija svim radnicima Instituta. Otvaranjem osobne poslovne adrese radnik automatski postaje dio zajedničke liste.
Prestankom radnog odnosa, uz brisanje korisničkog računa briše se i elektronička adresa i sadržaj elektroničkog poštanskog sandučića.
Bivši radnici koji su zadržali korisnički račun, ne mogu biti dio zajedničke adrese svi@iptpo.hr, osim ako ravnatelj ne odluči drugačije.
Izbrisana elektronička pošta ne čuva se.

Članak 10.

Radnici Instituta trebaju komunicirati elektroničkom poštom na način da se izbjegne nanošenje štete Institutu.

Pri korištenju elektroničke pošte radnici trebaju imati u vidu sljedeće:

1. Nesigurnost protokola
    - Lako je krivotvoriti adresu pošiljatelja.
    - Pri slanju i čitanju pošte poruke putuju kao običan tekst i moguće ih je presresti i pročitati.

2. Nepažnja korisnika
    - U žurbi se lako pritisne pogrešna tipka ili se klikne na susjednu ikonu. Time može nastati nepopravljiva šteta – ne možete zaustaviti poruku koja je već otišla.
    - . Nepažnjom se može prihvatiti adresa slična onoj koju zapravo tražite.

3. Nesporazumi
    - Elektronička pošta se često piše ležerno i neobavezno. Službene dopise treba pisati pažljivo i odmjereno.
    - Iza imena radnika u adresi elektroničke pošte nalazi se naziv ustanove za koju radi. Moguće je shvatiti privatno mišljenje radnika kao službeni stav Instituta.

4. Otkrivanje informacija
    - Poruke koje radnik uputili jednoj osobi, ona može proslijediti dalje. To se može dogoditi
        - (zlo)namjerno, s ciljem da se naškodi drugoj osobi ili tvrtki
        - nemarom primatelja, koji ne traži dozvolu za prosljeđivanje poruke
        - nenamjerno, na primjer nehotičnim klikom mišem na pogrešnu ikonu (*Odgovori svima umjesto Odgovori*)

5. Povrede autorskih prava
    - Svaka poruka elektroničke pošte može se, kao dovršen dokument, smatrati autorskim djelom. Prosljeđivanje poruke trećoj strani bez dozvole autora odnosno vlasnika smatra se povredom autorskog prava.
    - Prilozi koji se šalju uz elektroničke poruke mogu sadržavati autorski zaštićene informacije, na pr. glazbu, članke itd.

6. Prijenos štetnog softvera i neželjenih poruka
    - Elektronička pošta najčešći je način širenja virusa.
    - Neželjene komercijalne poruke, spam, oduzimaju dragocjeno radno vrijeme i nepotrebno opterećuju računala i mrežu.

Članak 11.

Zbog svega navedenog u prethodnom članku ovog Pravilnika korištenje elektroničke pošte smatra se rizičnom djelatnošću te se radnici obvezuju na pridržavanje slijedećih pravila:

- Institut daje radnicima e-mail adresu radi službene komunikacije.
- Službeni e-mailovi koriste se samo za službene svrhe, za obavljanje posla.
- Svaki dopis ili poruka s adrese koja završava sa @iptpo.hr može se shvatiti kao službeni dopis ili poruka, a osobni stav pošiljatelja kao službeni stav Instituta. Zato radnici, kada službene e-mail adrese koriste za privatnu svrhu, dužni su na porukama koje šalju označiti „privatno“, kako ne bi bilo dvojbe oko sadržaja poruke. Također, trebaju zatražiti od osoba od kojih očekuju privatne poruke na službenu e-mail adresu, da kao predmet poruke označe „privatno“. Oznaka „privatno“ jamči da Institut neće provjeravati sadržaj tih poruka bez posebnih razloga navedenih u ovom Pravilniku.
- Korisnici se moraju uzdržavati postupaka koji bi Institutu nanijeli materijalnu ili nematerijalnu štetu.

- Mora se paziti da se ne otkriju povjerljivi osobni ili poslovni podaci. Ukoliko poruka sadrži povjerljive informacije, treba je kriptirati i potpisati, a u sadržaju poruke jasno naznačiti da se radi o povjerljivim informacijama.
- Pri autentikaciji radi pristupa porukama potrebno je u IMAP/POP protokolu uključiti enkripciju, kako bi se spriječila mogućnost otkrivanja korisničkih lozinki.
- Nije dozvoljeno slanje neželjenih masovnih poruka, jer se primateljima oduzima dragocjeno vrijeme i neracionalno troše mrežni i računalni resursi.
- Korisnici su dužni oprezno rukovati s prispjelim porukama sumnjiva sadržaja, ne otvarati sumnjive priloge, ne *klikati* na sumnjive linkove itd. U slučaju sumnje, treba zatražiti pomoć osobe zadužene za informacijsku sigurnost (sistem inženjer).

Članak 12.

Poslovne poruke elektroničke pošte smatraju se službenim dokumentima.

Članak 13.

Institut zadržava pravo pregledavanja dolaznih i odlaznih poruka specijaliziranim programima radi zaustavljanja virusa i spama.

Članak 14.

Institut može poduzeti mjere za praćenje dopisivanja putem službenog e-maila i drugih vrsta komunikacija.
Radnici moraju biti upoznati s pravom Instituta navedenom u prethodnom stavku.
Institut može primarno pratiti tijek komunikacija - vrijeme slanja i primanja, e-mail adrese na koje se pošta šalje i s kojih se prima, a radi kontrole izvršenja posla, provjere je li pošta poslana službenim kontaktima i nadležnim tijelima te je li od istih primljena.
Radi obavijesti trećima s kojima radnici službeno stupaju u kontakt, u zaglavlju službene elektroničke poruke navodi se programska obavijest: „Ova elektronička pošta može biti predmet nadzora.“

Članak 15.

Institut može provjeravati sadržaj e-mailova isključivo u iznimnim okolnostima i to ako vrijednost dobra koje se želi zaštititi nadzorom i stupanj ugroze koji mu prijeti prevladava nad potrebom zaštite privatnosti, a posebice ako postoji opravdana sumnja u:

-odavanje poslovnih tajni Instituta
-odavanje osobnih podataka drugih radnika ili službenih kontakt osoba
-kršenje zabrane konkurencije Institutu
-narušavanje ugleda Instituta, iznošenje kleveta i neistina o Institutu
-korespondenciju u vezi drugih radnika koja može predstavljati vrijeđanje, uznemiravanje, spolno uznemiravanje ili diskriminaciju
-opasnosti po štetne posljedice za Institut
-sigurnosne incidente
-mobbing
-i druge povrede radne dužnosti.
Institut provjeru sadržaja može učiniti i kada je radnik odsutan, ako se radi o nužnoj kontroli primitka ili slanja e-mailova bitnih za poslovanje.

Članak 16.

Institut će primarno provjeru elektroničke pošte raditi uz pristanak i prisutnost službenika za zaštitu osobnih podataka, radnika koji se koristi e-mailom kojeg se provjerava te uz prisutnost još jednog radnika kao svjedoka.

Ako radnik ne da pristanak, ili radnik nije prisutan, ili ako okolnosti slučaja nužno zahtijevaju nadzor bez radnika, Institut će o nadzoru uvijek obavijestiti službenika za zaštitu osobnih podataka i još jednog radnika kao svjedoka pa podatke provjeriti zajedno s njima. Ako službenik za zaštitu osobnih podataka to odbije ili ako nije prisutan, a zbog opravdane hitnosti to je nužno učiniti, Institut će nadzor provesti uz prisutnost dva radnika kao svjedoka. O provođenju nadzoru vodi se zapisnik.

Institut će primarno provjeravati elektroničku poštu koja je službena odnosno onu kod koje iz adrese pošiljatelja ili primatelja ili iz naziva predmeta proizlazi da je službena te elektroničku poštu za koju se ne vidi je li privatna ili nije.

Za elektroničku poštu koja je označena kao privatna, sadržaj će se provjeriti samo iznimno, u slučaju ako je upravo takva pošta ona koja može Institutu dati navedeni podatak zbog kojeg ima opravdani razlog za provjeru takve pošte.

Pri provjeri sadržaja e-mailova, osobito onih koji bi mogli biti privatni, napravit će se najkraći mogući pregled, izbjegavajući dobivanje više informacija od onog što je nužno.

U provjeri elektroničke pošte, u slučaju potrebe za tehničkom podrškom, iznimno može sudjelovati i stručna osoba bez koje provjera ne bi bila moguća (sistem inženjer).

Članak 17.

Sve osobe koje sudjeluju u provjeri pošte dužne su podatke privatne naravi koje saznaju putem nadzora elektroničke pošte čuvati kao tajne i nigdje i nikome ih ne smiju iznositi.

Iznimno, odredba st. 1. ovog članka ne odnosi se na podatke koji su bili razlog za nadzor i koji predstavljaju kršenje propisa ili ugovornih obveza.

U odnosu na podatke koji se na prethodni način saznaju, a koji predstavljaju uznemiravanje i/ili spolno uznemiravanje, u daljnjem postupku poštivat će se tajnost podataka sukladno Zakonu o radu.

Članak 18.

Sav nadzor iz članka 14.-16. ovog Pravilnika vremenski je ograničen samo za slučaj za koji je proveden i nakon toga se više ne provodi, osim ako se takav slučaj ne ponovi.

Nadzor iz čl. 14.-16. ovog Pravilnika Institut će provoditi isključivo kao krajnju mjeru kada postoje opravdane sumnje u ozbiljno kršenje propisa ili ugovornih obveza, osobito ono koje može dovesti do štete za Institut i/ili druge osobe te kada se drugim postupcima ne može doći do rezultata.

Podaci o počinjenju povrede radne obveze za koje se saznalo nadzorom službenog e-maila mogu se koristiti kao dokaz u eventualnim daljnjim postupcima (disciplinski, sudski i sl.)

Pisma i paketi

Članak 19.

Pošta (pisma, paketi i dr.) koja dolazi u sjedište Instituta s naznačenom adresom Instituta, smatra se poštom Instituta, neovisno o tome je li pored naziva i adrese Instituta naznačeno ime radnika na kojega se ta pošta odnosi.

Privatnom poštom radnika smatrat će se ona na kojoj je to naznačeno, odnosno kod koje se iz svih okolnosti vidi da se radi o privatnoj pošti.

Članak 20.

Svu poštu dostavljenu Institutu otvara, urudžbira i razvrstava osoba zadužena za poštu.

Pošta se neće otvoriti ako je na njoj izričito označeno da se radi o privatnoj pošti (oznaka „privatno“) ili ako to proizlazi iz okolnosti slučaja (npr. pošiljatelj je član obitelji radnika) i tada će se takva pošta neotvorena predati radniku.

Članak 21.

Ako radnik očekuje privatnu poštu na adresu Instituta, dužan je o tome obavijestiti osobu zaduženu za poštu, s napomenom podataka o pošiljatelju, kako ne bi zabunom došlo do otvaranja te pošte.

U slučaju da osoba zadužena za poštu otvori privatnu poštu radnika, jer se nije moglo vidjeti da se radi o privatnoj pošti, ne smije dalje istu čitati ni provjeravati, nego je treba odmah uručiti radniku, a eventualne podatke iz pošte koje je vidio čuvati kao tajnu.

Službeni telefoni i mobiteli

Članak 22.

Službeni telefoni i mobiteli vlasništvo su Instituta i koriste se primarno za službene potrebe.

Dopušteno je korištenje službenog telefona i mobitela za privatne potrebe, ali vodeći računa da se time ne ometa proces rada, da u radno vrijeme takvi razgovori ne predstavljaju znatni utrošak radnog vremena i da se Institutu ne stvaraju prekomjerni troškovi.

Zabranjeno je korištenje službenih telefona i mobitela za zvanje u privatne svrhe brojeva koji se dodatno naplaćuju.

Zabranjeno je korištenje službenih telefona i mobitela za namjene protivne interesima Instituta, a posebice za one iz čl. 15. ovog Pravilnika.

Drugi oblici komunikacije

Članak 23.

Odredbe ovog Pravilnika na odgovarajući način se primjenjuju na sve druge oblike komunikacije koje nisu uređene Pravilnikom (npr. telefax i sl).

Završne odredbe

Članak 24.

Prilikom prikupljanja, pohranjivanja, čuvanja i korištenja podataka prikupljenih nadzorom komunikacije, Institut je dužan zaštiti podatke sukladno zakonskim i podzakonskim aktima kojima se regulira zaštita osobnih podataka, kao i drugim važećim propisima kojima se uređuje to područje.

Pristup podacima dobivenim nadzorom obavljenim na temelju ovog Pravilnika te ovlaštenje za obradu osobnih podataka imaju ravnatelj Instituta i osoba ili osobe koje on posebnom odlukom na to ovlasti.

Podaci dobiveni nadzorom smiju se koristiti isključivo za svrhe za koje je nadzor određen te se podaci o osobama prikupljeni nadzorom ne smiju koristiti izvan njihove određene i zakonske namjene, a raspolaganje podacima dopušteno je samo ravnatelju odnosno osobi koju on za to ovlasti.

Osobe iz st. 1. i 2. ovog članka, kao i sistem inženjer, ukoliko je prisustvovao nadzoru, pisanom izjavom obvezat će se na povjerljivost osobnih podataka za koje saznaju provođenjem nadzora.
Svi podaci dobiveni iznimnim nadzorom čuvaju se najdulje 30 dana, nakon čega se trajno brišu, a iznimno se mogu čuvati duže, koliko je to nužno za potrebe sudskog ili drugog postupka.
Nadzor nad korištenjem nadzora i obradom podataka ima osoba određena sukladno članku 29. stavak 6. Zakonu o radu i službenik za zaštitu osobnih podataka.
Radnici i druge osobe čiji se osobni podaci prikupe temeljem nadzora iz ovog Pravilnika, mogu sve informacije o provođenju nadzora dobiti od osoba iz st. 2. i 6. ovog članka, mogu od tih osoba tražiti pristup osobnim podacima i ispravak, brisanje ili prijenos osobnih podataka, ili ograničavanje obrade koji se na njih odnose te imaju i pravo na ulaganje prigovora na nadzor i obradu podataka.
Osoba koja smatra da joj je povrijeđeno neko pravo zajamčeno propisima o zaštiti osobnih podataka, može podnijeti prigovor Institutu koji kao voditelj obrade ima dužnost donijeti odluku u roku od mjesec dana. Prigovor se podnosi službeniku za zaštitu osobnih podataka. U slučaju neslaganja s odlukom Instituta, osoba može Agenciji za zaštitu osobnih podataka podnijeti zahtjev za utvrđenje povrede prava.

Članak 25.

Ovaj Pravilnik stupa na snagu osmog dana od dana objave na oglasnoj ploči Instituta.

URBROJ: 0147-18-179
Poreč, 24. rujna 2018.

Predsjednica Upravnog vijeća

prof. dr. sc. Tajana Krička

Ovaj Pravilnik objavljen je na oglasnoj ploči Instituta 25. 9. 2018., a stupio je na snagu 3. 10. 2018..

Ravnatelj

dr. sc. Dean Ban