POLJOPRIVREDNI INSTITUT OSIJEK

PRAVILNIK

O SIGURNOSTI INFORMACIJSKIH SUSTAVA

Osijek, 2021.

Na temelju članka 26., 63. i 65. Statuta Poljoprivrednog instituta Osijek (pročišćeni tekst: 2014.), Upravno vijeće Poljoprivrednog instituta Osijek na IX. sjednici održanoj dana 20.12.2021. donosi

PRAVILNIK O SIGURNOSTI INFORMACIJSKIH SUSTAVA POLJOPRIVREDNOG INSTITUTA OSIJEK

I. OPĆE ODREDBE

Članak 1.

(1) Pravilnikom o sigurnosti informacijskih sustava Poljoprivrednog instituta Osijek (u daljnjem tekstu: Pravilnik) uređuje se sigurnost upravljanja informacijskim sustavima na Poljoprivrednom institutu Osijek (u daljnjem tekstu: Institut) i sigurnosna politika, definiraju se prihvatljivi načini ponašanja i jasna raspodjela uloga i odgovornosti svih čimbenika informacijskog sustava.

(2) Informacijski sustav mora omogućiti nesmetano odvijanje poslovnih procesa kroz uporabu informacija. Obavljanje poslovnih procesa Instituta ovisi o radu informacijskog sustava Instituta.

(3) Sigurnost informacijskog sustava definira se kao skup mjera i postupaka, na tehničkoj i organizacijskoj razini, čijom se primjenom postiže i održava prihvatljiva razina rizika informacijskog sustava.

(4) Institut može usvojiti i druge dokumente kojima se specificiraju pojedine odredbe programa sigurnosti.

(5) Sigurnosna politika treba biti planirana i provedena na način da se omogućava sigurno obavljanje posla, a da pritom ne ometa poslovne procese.

Članak 2.

Izrazi koji se koriste u ovom Pravilniku, a imaju rodno značenje, koriste se neutralno i odnose se jednako na muški i ženski rod.

II. POJMOVI I TERMINI

Članak 3.

(1) Informacijski sustav (u daljnjem tekstu: IS) podrazumijeva usklađeno djelovanje svojih sastavnica i komponenti:

- računalne i komunikacijske tehnologije,

- sistemskog i aplikativnog softvera,
- podataka/informacija,
- metoda i postupaka za obradu podataka,
- osoba koje održavaju IS, obrađuju podatke i koriste ih,
- poslovnih partnera i suradnika.

(2) Informacijsku imovinu sačinjava svaki resurs IS koji služi za prikupljanje, obradu, spremanje ili distribuciju podataka, na primjer:

- opipljiva (materijalna) imovina (zgrade, računala i komunikacijska oprema, infrastruktura),
- neopipljiva (nematerijalna) imovina (ugled, tehnologija, metodologija, zaštitni znak),
- podaci (dokumenti, ugovori, osobni podaci, itd.),
- softver (sistemski i aplikativni programski paketi),
- ljudi koji održavaju i koriste IS.

(3) Temeljna načela sigurnosti informacijskog sustava su:

- povjerljivost - informacije su dostupne samo ovlaštenim ljudima i organizacijama,
- cjelovitost - ažurnost i točnost podataka, sprečavanje neovlaštenog mijenjanja i uništavanja podataka,
- dostupnost - podaci moraju biti na raspolaganju ovlaštenim korisnicima u trenutku kada su potrebni.

(4) Procjena rizika je postupak kojima se identificiraju prijetnje i ranjivosti koje mogu ugroziti rad informacijskog sustava.

- Za svaku prijetnju određuje se vjerojatnost ostvarenja i potencijalna šteta, kako bi se odredili prioriteti i odabrale mjere koje smanjuju rizik na prihvatljivu razinu.
- Procjena rizika provodi se periodički kako bi se ustanovile promjene u prijetnjama, ranjivosti i poslovnim prioritetima.
- Troškovi primjene sigurnosnih mjera moraju biti razmjerni s osjetljivošću i vrijednošću informacija koje se takvim mjerama štite i prilagodeni materijalnim i ljudskim mogućnostima.

(5) Sigurnosni događaj je svaki događaj koji ukazuje na problem koji ne ugrožava rad samog informacijskog sustava niti povjerljivost podataka (na primjer: kada korisnici zaborave zaporku).

(6) Sigurnosni incident je događaj koji ugrožava povjerljivost, integritet i dostupnost podataka, integritet sistemskog softvera i poslovnih aplikacija ili ukazuje na neovlašteni pristup informacijskim resursima. Incidentom se smatraju i događaji koji su onemogućili neprekidnost poslovanja, poput nestanka električne energije, poplava, požara, itd.

III. OPSEG PRIMJENE

Članak 4.

(1) Pravila rada i ponašanja koja su definirana sigurnosnom politikom odnose se na:
- svu računalnu opremu koja se koristi u prostorima Instituta,
- administratora informacijskih sustava,
- korisnike (zaposlenici, vanjski suradnici, i dr.)
- vanjske tvrtke koje po ugovoru rade na održavanju opreme ili softvera.

(2) Politika sigurnosti primjenjuje se na sve komponente informacijskog sustava.

(3) Pravila sigurnosne politike dužni su poštivati i provoditi ih svi zaposlenici, poslovni parterni i vanjski suradnici koji imaju pristup podacima i informacijskoj infrastrukturi u skladu s poslovnim potrebama.

(4) Novi zaposlenici dužni su se upoznati sa odredbama ovog Pravilnika prilikom zapošljavanja.

IV. ORGANIZACIJA UPRAVLJANJA SIGURNOŠĆU

Članak 5.

(1) Osobe koje se u radu koriste računalima i ostalim uređajima koji se priključuju na IS dijele se na pružatelje i korisnike informatičkih usluga.

(2) Pružatelji informatičkih usluga su osobe koje su zadužene za ispravnost i neprekidnost rada računala, mreže i IS. Samo pružatelj smije biti administrator računala koja se koriste na Institutu.

Administratori računala dužni su se upoznati sa odredbama ovog Pravilnika i potpisati Izjavu o prihvaćanju odredbi sigurnosne politike. (prilog 1. i prilog 2. Pravilnika)

(3) Korisnici informatičkih usluga su osobe koje se u svom radu ili izobrazbi koriste računalima, komunikacijskim uređajima i svim ostalim uređajima koji se priključuju na IT infrastrukturu Instituta, u svrhu proizvodnje dokumenta, unosa podatke ili koriste informatičke usluge Instituta, ali ne odgovaraju za instalaciju i konfiguraciju softvera, niti za ispravan i neprekidan rad računala i mreže.

Korisnikom se smatra svaki zaposlenik, vanjski partner ili dr. osoba koji u skladu s poslovnim potrebama pristupa informacijskom sustavu Instituta.

(4) Korisnik informatičkih usluga obvezuje se:
- pridržavati pravila prihvatljivog korištenja, ne koristiti računala za radnje koje nisu u skladu sa važećim zakonima, etičkim i moralnim normama i sigurnosnom politikom Instituta,
- pridržavati odredbi ovog Pravilnika,

- izabrati kvalitetnu zaporku, osigurati sigurno korištenje i čuvanje zaporki te ju povremeno mijenjati,
- čuvati autentifikacijske atribute za pristup računalima i komunikacijskim uređajima na siguran način i ne otkrivati ih drugim osobama ni pod kojim uvjetima,
- prijaviti svaki sigurnosni incident,
- ukoliko u svom radu proizvodi podatke i dokumente, odgovoran je za vjerodostojnost tih podataka te za njihovo čuvanje kao i za izradu sigurnosnih kopija podataka,
- u slučaju oštećenja ili kvara računala i/ili komunikacijskog uređaja prijaviti administratoru Instituta u što je moguće kraćem roku,
- u slučaju krađe ili gubitka računala i/ili komunikacijskog uređaja prijaviti predstojniku ustrojstvene jedinice u što je moguće kraćem roku,
- omogućiti neometani rad prilikom održavanja računala i/ili komunikacijskih uređaja pružateljima informatičkih usluga,
- prilikom uporabe Interneta ne upuštati u aktivnosti koje su zakonom određene kao nelegalne,
- izbjegavati aktivnosti koje bi mogle ugroziti sigurnost njihovih računala i informacijskog sustava Instituta,
- koristiti službenu elektroničku poštu Instituta kao službeno sredstvo komunikacije, vodeći računa o čuvanju ugleda Instituta prilikom sastavljanja iste te biti svjestan da korištenje elektroničkih poruka ne podrazumijeva privatnost i sigurnost samih poruka,
- u slučaju dobivanja sumnjive elektroničke pošte postupati s razumnim oprezom te ne slijediti linkove i ne otvarati priloge koji se nalaze u elektroničkoj poruci, ukoliko je vjerodostojnost pošiljatelja upitna. O svim takvim porukama potrebno je odmah obavijestiti administrator Instituta.

Korisnicima je zabranjeno:

- isključivanje i ometanje rada sustava za nadzor, upravljanja i zaštite računala te isključivanja ili onemogućavanja programa za zaštitu od virusa,
- neovlašteno kopiranje na računalo materijala koje je zaštićeno pravom intelektualnog vlasništva, zaštićenih fotografija, tekstova, filmova, glazbe, programa, ...
- namjerno unošenje malicioznih programa u mrežne sustave i servere (npr: virusi, crvi, trojanski konji, ...),
- odavanje svoje lozinke drugim osobama ili dopuštanje uporabe vlastitog korisničkog računa (user account) drugim osobama, neovisno o tome jesu li te osobe zaposlenici Instituta,
- namjerno uzrokovanje sigurnosnih incidenata, pristupanje podacima koji nisu namijenjeni korisniku ili korisničkom računu za koji korisnik nema dozvolu za uporabu,
- neovlašteno konfiguriranje ili onemogućavanje/prekidanje rada mrežne i komunikacijske opreme,
- zaobilaženje autentifikacije i sigurnosnih mjera za pristup bilo kojem dijelu IS,
- neovlašteno dodavanje/mijenjanje hardverske konfiguracije sustava ili dijela sustava (računala),
- neovlašteno mijenjanje sigurnosnih postavki računala i komunikacijskih uređaja,
- neovlašteno instaliranje programa,
- instaliranje i uporaba softvera na način da se krše prava intelektualnog vlasništva,

- korištenje neovlaštenih programa koji ne zahtijevaju instalaciju ("portabilnih aplikacija") na računalu,
- slanje poruka koje sadrže podatke ili informacije protivno važećim sigurnosnim pravilima Instituta,
- slanje poruka nedoličnog, lažnog i uvredljivog sadržaja te poruka s obmanjujućim sadržajem,
- uznemiravanje putem elektroničke pošte u bilo kojem obliku kao npr. slanje velike količine neželjenih ili nezatraženih elektroničkih poruka na jedan korisnički račun,
- slanje ili prenošenje sadržaja koji nude usluge ili proizvode u obliku lančanih pisama,
- lažno predstavljanje ili davanje korisničkog imena i lozinke drugoj osobi, čime se omogućuje lažno predstavljanje, krivotvorenje zaglavlja poruke,
- objavljivanje sadržaja na Internetu bez suglasnosti vlasnika sadržaja te objavljivanje ili prenošenje netočnih, nepotpunih i uvredljivih podataka ili informacija,
- uporaba računala i komunikacijskih uređaja za neautorizirani pristup drugim računalima, mreži ili komunikacijskim uređajima preko Interneta ili ometanje drugih računala na Internetu.

(5) Korisnici su odgovorni za profesionalno, etičko i zakonito korištenje računalnih resursa koji su im dani na raspolaganje prvenstveno za korištenje u svrhe poslovnih procesa Instituta.

(6) S obzirom da kapaciteti mrežnih i računalnih resursa Instituta imaju svoja ograničenja, od svih korisnika se očekuje korištenje računalnih resursa učinkovito i racionalno te na način koji neće onemogućiti ili smanjiti efikasnost rada drugih korisnika.

Članak 6.

Dokumenti u elektroničkom obliku smatraju se službenim dokumentima na isti način kao i dokumenti na papiru te treba osigurati njihovo čuvanje i pristup samo ovlaštenim osobama.

Članak 7.

(1) Pružatelji informatičkih usluga dužni su administrirati računala i mrežnu opremu u skladu s pravilima struke, brinući istovremeno o funkcionalnosti i sigurnosti cjelokupnog IS.
Imenovani administrator Instituta odgovoran je za instalaciju i konfiguraciju softvera na računalima u vlasništvu Instituta.

(2) Računala se moraju konfigurirati na način da budu zaštićena od napada izvana i iznutra, što se osigurava instaliranjem softverskih zakrpi po preporukama proizvođača, listama pristupa, filtriranjem prometa i drugim sredstvima.

(3) Administrator Instituta dužan je posebnu pažnju posvetiti opremi koja obavlja ključne funkcije ili sadrži vrijedne i povjerljive informacije koje treba štiti od neovlaštenog pristupa.

(4) Pružatelji informatičkih usluga ne smiju administrirati računala i mrežnu opremu koja je u vlasništvu privatnih i poslovnih korisnika.

(5) Pružatelji informatičkih usluga dužni su u svome radu poštivati privatnost ostalih korisnika i povjerljivost informacija s kojima dolaze u dodir pri obavljanju posla.

Članak 8.

(1) Administrator Instituta svakodnevno prati rad sustava, čita dnevničke zapise i provjerava rad servisa. Zadaća je administratora i nadgledanje rada korisnika, kako bi se otkrile nedopuštene aktivnosti.

(2) Administrator Instituta dužan je prijaviti incidente ravnatelju Instituta te pomoći pri istrazi i uklanjanju problema. Incidenti se dokumentiraju kako bi se pomoglo u nastojanju da se izbjegnu slične situacije u budućnosti. U koliko je incident ozbiljan i uključuje kršenje zakona Republike Hrvatske, prijavljuju se CARNetovu CERT-u.

Članak 9.

(1) Upravljanje mrežom, konfiguriranje mrežnih uređaja, dodjeljivanje mrežnih adresa, kreiranje virtualnih LAN-ova te ostale poslove pri upravljanju mrežom vrši administrator Instituta.

(2) Zahtjev za priključivanje računala na mrežu daje se isključivo administratoru Instituta koji provodi daljnje korake za priključivanje računala na mrežu.

(3) Administrator Instituta je dužan voditi Popis mrežnih priključaka i umreženih uređaja, uključujući i prenosiva računala. Administratori CARNet-ovih poslužitelja dužni su voditi Popis javnih adresa računala.

Članak 10.

Spajanje na mrežu gostujućih računala koja donose sa sobom vanjski suradnici, predavači, poslovni partneri, serviseri dopušteno je samo uz dopuštenje ravnatelja Instituta i uz nadzor administratora Instituta.

Članak 11.

(1) Korištenje ilegalnog softvera predstavlja povredu autorskog prava i intelektualnog vlasništva. Ravnatelj Instituta zadužuje odgovornu osobu za instaliranje softvera i njegovo licenciranje.

(2) Korisnik koji ima potrebu za nekim programom/aplikacijom, mora se obratiti ravnatelju Instituta i zatražiti, uz obrazloženje, nabavu i instalaciju istog.

(3) Radi poboljšanja sigurnosti, za svaki instalirani program/aplikaciju koja služi obradi podataka imenuje se glavni korisnik. Glavni korisnik odgovoran je za ispravnost i sigurnost programa/aplikacije, za dodjelu dozvola za pristup, unos i izmjenu podataka te je odgovoran za provjeru ispravnosti podataka.

(4) Glavni korisnik kontaktira proizvođača aplikacije i dogovora isporuku novih verzija te traži ugradnju sigurnosnih mehanizama uz pomoć i nadzor od strane administratora Instituta.

V. FIZIČKA SIGURNOST INFORMATIČKOG SUSTAVA

Članak 12.

(1) Prostor na Institutu dijeli se na dio koji je otvoren za javnost, prostor u koji imaju pristup samo zaposleni te prostore u koje pristup imaju samo grupe zaposlenih ovisno o vrsti posla koji obavljaju.

(2) Administrator Instituta vodi i održava popis osoba koje imaju pristup u zaštićena područja (tzv. serverska soba), a osoba na portirnici mora imati popis osoba koje mogu dobiti ključeve određenih prostorija.

(3) Opće smjernice vezane uz fizičku sigurnost:

1. zaključavanje ureda i ormara s dokumentima;
2. računalni sustavi koji se koriste za pristup osjetljivim podatcima moraju se instalirati samo ondje gdje su dostupni ovlaštenim zaposlenicima;
3. svi korisnici moraju poduzeti primjerene mjere opreza da bi osigurali da drugi korisnici ne mogu neovlašteno pristupati podatcima koristeći njihovu opremu te ne smiju pristupati opremi koristeći tuđe korisničko ime;
4. pristup informacijama mora odobriti administrator Instituta te po potrebi ravnatelj Instituta ovisno o kojem izvoru informacijama se radi;
5. sva oprema i mediji za otpis moraju se razdužiti na propisani način. Osjetljivi podatci i softver koji ima neprenosivu licencu mora se potpuno izbrisati s diska;
6. svi osjetljivi i povjerljivi tiskani zapisi moraju se isjeckati prije odlaganja;
7. oprema, podaci i softver u vlasništvu Instituta ne smije se iznositi iz službenih prostora bez službenog odobrenja;
8. ako se oprema koristi izvan prostora Instituta za obradu osjetljivih podataka, na nju se odnose iste mjere opreza kao i za opremu korištenu unutar prostora;
9. oprema i mediji koji sadrže osjetljive informacije ne smiju se ostavljati bez nadzora na javnim mjestima niti na vidljivom mjestu unutar automobila. Prenosiva računala moraju se nositi kao ručna prtljaga. Opremu je potrebno zaštiti zaporkom;
10. korisnici ne smiju izrađivati neovlaštene kopije softvera u vlasništvu Instituta osim u slučajevima kada je navedeno zakonom dopušteno ili kada to odobri vlasnik. Regulacijom intelektualnog vlasništva propisane su posljedice kopiranja originalnih podataka i softvera te će za njih odgovarati korisnik.

Članak 13.

(1) Oprema koja obavlja kritične funkcije, neophodne za funkcioniranje IS ili sadržava povjerljive informacije, fizički se odvaja u prostor u koji je ulaz dozvoljen samo ovlaštenim osobama (u daljnjem tekstu: sigurna zona).

(2) Administrator Instituta dužan je održavati popis ovlaštenih osoba koje imaju pristup u sigurnu zonu. U pravilu su to samo zaposlenici i vanjski suradnici koji administriraju mrežnu i komunikacijsku opremu i poslužitelje ključnih servisa. Oni ulaze u sigurnu zonu samo kada treba ukloniti zastoje, obaviti servisiranje opreme, zamijeniti postojeću opremu novom, itd.

(3) Povremeno se mora dopustiti pristup sigurnoj zoni osobama iz vanjskih tvrtki ili ustanova radi servisiranja, održavanja, podrške, obuke, zajedničkog poslovanja, konzultacija i itd.

(4) Institut može zahtijevati da se svaka osoba koja pristupa povjerljivoj opremi. sigurnoj zoni ili osjetljivim informacijama upozna sa odredbama ovog Pravilnika i potpiše Izjavu o čuvanju povjerljivih informacija. (prilog 2.)

(5) Institut je dužan osoblju CARNeta dozvoliti pristup opremi u vlasništvu CARNeta koja se nalazi na Institutu.

(6) Kritična oprema treba biti zaštićena od problema s napajanjem električnom energijom, poplava, požara i sl. te treba poduzeti mjere da se oprema i informacije zaštite i da se osigura što brži oporavak. U sigurnoj zoni i u njihovoj blizini ne smiju se držati zapaljive i eksplozivne tvari.

VI. SIGURNOST OPREME

Članak 14.

Institut dijeli svu opremu u grupe prema zadaćama:

- zona javnih servisa - oprema koja obavlja javne servise (DNs poslužitelj, web poslužitelj, poslužitelj elektroničke pošte, itd.),
- intranet - privatna mreža Instituta (poslužitelji internih servisa, osobna računala zaposlenika, komunikacijska oprema lokalne mreže, itd.),
- extranet - proširenje privatne mreže na mobilne korisnike, poslovne partnere ili na izdvojene lokacije (interni modemski ulazi, veze lokalnih baza podataka sa središnjim poslužiteljima, itd.).

Članak 15.

(1) U prostorijama Instituta nalazi se i oprema CARNeta ili nadležnog ministarstva koja je dana na korištenje Institutu.

(2) Institut je obvezan održavati popis sve računalne opreme s opisom ugrađenih komponenti, inventurnim brojevima i itd.

(3) Institut jednako brine o svoj opremi kojom raspolaže bez obzira na to tko je njezin vlasnik te je čuva od oštećivanja i otuđenja pažnjom dobrog gospodara.

Članak 16.

(1) Za fizičku sigurnost opreme za infrastrukturu koja je u vlasništvu Instituta odgovoran je ravnatelj Instituta.

(2) Ravnatelj Instituta odgovornost za grupe uređaja ili pojedine uređaje prenosi na druge zaposlene, koji potpisuju dokument kojim potvrđuju da su preuzeli opremu.

(3) Računala i računalna oprema daje se korisnicima na raspolaganje radi obavljanja poslova vezanih uz izvršenje radnih obveza korisnika i redovne djelatnosti Instituta te ju nije dopušteno koristiti za obavljanje privatnih poslova.

(4) Privatna računala i računalnu opremu nije dopušteno priključivati na fiksnu računalnu mrežu Instituta osim uz odobrenje administratora Instituta i ravnatelja Instituta.

(5) Računala i računalnu opremu nije dopušteno iznositi izvan prostora Instituta bez prethodnog odobrenja predstojnika ustrojstvene jedinice. Navedeno ne uključuje prijenosna računala u vlasništvu Instituta za koje postoji Potvrda o zaduživanju (u prilogu 3.).

(6) Korisnici koji opremu koriste izvan prostora Instituta odgovorni su za tu opremu kao i za sve posljedice koje proizlaze iz korištenja iste.

VII. OSIGURANJE NEPREKIDNOSTI POSLOVANJA

Članak 17.

(1) Kako bi se sačuvali podaci u slučaju nezgoda, poput kvarova na sklopovlju, požara ili ljudskih grešaka, potrebno je redovito izrađivati rezervne kopije svih podataka važnih za održavanje vitalnih funkcija informacijskog sustava i sklopovlja.

(2) Stavak 1. ovog članka prvenstveno se odnosi na kopije sustava središnjih poslužitelja, knjižničkog poslužitelja, računovodstvenih podataka i podataka o konfiguraciji softvera neophodnog za funkcioniranje mreže.

Članak 18.

(1) Za izradu rezervnih kopija podataka središnjih poslužitelja zaduženi su CARNet sistem inženjeri koji administriraju te poslužitelje. Za neprekidnost rada središnjeg poslužitelja odgovoran je administrator istog poslužitelja.

(2) Za izradu rezervnih kopija podataka važnih za održavanje vitalnih mrežnih funkcija i računala važnih za podršku korisnicima, nadležan je administrator Instituta.

(3) Za izradu rezervnih kopija računovodstvenih podataka zadužena je tvrtka s kojom Institut ima ugovor o održavanju programske podrške.

Članak 19.

Osobe zadužene za izradu rezervnih kopija dužne su povremeno provjeravati upotrebljivost rezervnih kopija podataka te izvoditi vježbe oporavka sustava. Vježbe je potrebno izvoditi na posebnim računalima i u posebnim uvjetima.

VIII. NADZOR NAD INFORMACIJSKIM SUSTAVIMA

Članak 20.

(1) CARNet ima pravo nadzora nad načinom korištenja CARNet mreže. U skladu s Pravilima prihvatljivog korištenja, CARNet može privremeno ili trajno uskratiti pravo korištenja CARNet mreže i njezinih servisa.

(2) Institut zadržava pravo nadzora nad radom korisnika i načinom korištenje računala i računalne opreme, instaliranim softverom i podacima koji su pohranjeni na umreženim računalima.

(3) Nadzor se smije provoditi radi:
- osiguranje integriteta, povjerljivosti i dostupnosti informacija i resursa,
- provođenja istrage u slučaju sumnje da se dogodio sigurnosni incident,
- provjere da li su IS i njihovo korištenje usklađeni sa zahtjevima sigurnosne politike.

Nadzor smiju obavljati samo osobe koje je ravnatelj Instituta za to ovlastio.

(4) Prilikom provođenja nadzora, ovlaštene osobe dužne su poštivati privatnost i osobnost korisnika te njihovih podataka.

(5) U slučaju da je korisnik prekršio pravila sigurnosne politike, povjerljivost informacija se ne mora osigurati i mogu se pregledati sav sadržaj na računalu, uključujući i onaj koji korisnik smatra privatnim i osobnim.

Članak 21.

Odredbe iz članka 20. ovog Pravilnika odnose se na sva računala i računalnu opremu koja se nalazi u prostorijama Instituta i priključena je u mreži CARNet-a, na instalirani softver te na mrežne servise.

Članak 22.

(1) Korisnici su dužni pomoći ovlaštenim osobama zaduženim za nadzor IS, pružiti sve potrebne informacije i omogućiti im pristup prostorijama i opremi. Isto vrijedi i za administratora Instituta i pojedinih servisa koji su ovlaštenim osobama dužni pomagati pri istrazi.

(2) Pristup uključuje:
- pristup na razini korisnika ili sustava na računalima i računalnoj opremi,

- pristup svim informacijama, u elektroničkom ili tiskanom obliku, koja je proizvedena ili spremljena na opremi Instituta ili oprema Instituta služi za njezin prijenos,
- pristup radnom prostoru (uredu, laboratoriju, sigurnoj zoni itd.),
- pravo na interaktivno nadgledanje i bilježenje prometa na mreži Instituta.

Članak 23.

Korisniku koji ne postupi po pravilima o nadzoru može se uskratiti pravo na korištenje CARNetove mreže i njezinih servisa te se otkrivene informacije u nadzoru mogu koristiti u sudskom postupku ili poduzimanju sankcija protiv korisnika sukladno važećim propisima.

IX. KORIŠTENJE RAČUNALA I RAČUNALNE OPREME INSTITUTA

Članak 24.

(1) Nedozvoljenim korištenjem računala i računalne opreme smatra se svako korištenje koje dovodi do povrede važećih zakona, propisa ili etičkih normi, a mogao bi izazvati materijalnu ili nematerijalnu štetu za Institut.

(2) Lakšim oblicima nedozvoljenog korištenja računala i računalne opreme smatra se:
- ograničena uporaba nelicenciranog softvera,
- skidanje (Download) autorski zaštićenih datoteka bez plaćanja naknade ako su iste javno dostupne,
- skidanje (download) i/ili distribucija sadržaja koji nije primjeren (pornografija i sl.),
- slanje masovnih poruka, bile one komercijalne prirode ili ne, čime se nepotrebno troše mrežni resursi,
- samovoljna instalacija softvera,
- korištenje neprihvatljivih aplikacija i servisa zbog kojih se narušava sigurnost informacijskih sustava, nepotrebno troše mrežni resursi ili se nanosi bilo kakva materijalna i/ili nematerijalna šteta Institutu,
- korištenje mrežnih resursa Instituta na način priključivanja vlastitih - privatnih računala na računalnu mreže Instituta.

(3) Težim oblicima nedozvoljenog korištenja računala i računalne opreme smatra se:
- preuzimanje tuđeg identiteta (korištenje opreme s tuđim korisničkim računom, slanje elektroničke pošte pod tuđim imenom, kupovanje preko internet s tuđom kreditnom karticom, itd.)
- provaljivanje na druga računala.
- traženje ranjivosti i sigurnosnih propusta; korisnik ne smije samoinicijativno skenirati računala, probijati zaporke ili na bilo koji način istraživati sigurnosne propuste na računalima, bilo da ona pripadaju Institutu ili ne,
- napad uskraćivanjem resursa na druga računala,
- vrijeđanje i ponižavanje osoba u internetskoj komunikaciji po spolnoj, vjerskoj, rasnoj, nacionalnoj ili nekoj drugoj pripadnosti.

Članak 25.

(1) Neprihvatljivim korištenjem računala i računalne opreme smatra se svako korištenje koje nije vezano uz obavljanje poslova i radnih zadataka korisnika i djelatnosti Instituta te svako drugo prekomjerno korištenje računala i računalne opreme koje ima za posljedicu neučinkovito korištenja radnog vremena i neizvršavanja preuzetih obveza iz ugovora o radu.

(2) Institut zadržava pravo procjene prihvatljivog, odnosno neprihvatljivog korištenja računala i računalne opreme.

(3) Ravnatelj Instituta će sankcionirati neprihvatljive oblike korištenja računala i računalne opreme, a posebice ako se radi o opetovanom i učestalom neprihvatljivom korištenju, a na prijedlog predstojnika ustrojstvene jedinice i na temelju procjene/mišljenja administratora Instituta i/ili drugi osoba imenovanih od strane ravnatelja Instituta sukladno članku 20. stavak 2 ovog Pravilnika.

(4) Korisnici informatičkih resursa i opreme dužni su upozoriti administratora Instituta i ravnatelja Instituta na svaki oblik neprihvatljivog ponašanja drugih korisnika, a prvenstveno su dužni svojim primjerom pozitivno utjecati na promicanje prihvatljivog ponašanja.

Članak 26.

(1) Zaposlenici Instituta, poslovni partneri, suradnici i/ili predavači na skupovima koje se održavaju u prostorijama Instituta sami su dužni voditi računa o ispravnosti i sigurnosti osobnih računala koje koriste za predavanja, na skupovima, radionicama i slično.

(2) Administrator Instituta niti jednog trenutka na preuzima odgovornost za eventualno nastalu štetu na osobnim računalima koja nisu konfiguriran u skladu sa odredbama ovog Pravilnika.

(3) Ukoliko administrator Instituta utvrdi kako oprema nije u skladu sa sigurnosnim zahtjevima IS Instituta i ista može prouzročiti štetu (virusi, spyware, malware, piratski softver, ...) istu neće spajati na mrežnu i ostalu infrastrukturu IS.

X. INTERNET I BEŽIČNA MREŽA

Članak 27.

(1) Internet se smatra značajnom komponentom IS Instituta te se može koristiti prije svega za poslovne namjene, informiranje i edukaciju.

(2) Administrator Instituta odgovoran je za provedbu odgovarajućih mjera kojima se onemogućuje neovlašten pristup unutarnjoj mreži ili podacima Instituta putem Interneta te je dužan osigurati provedbu mjera na tehničkoj i organizacijskoj razini kojom se smanjuju rizici korištenja Interneta.

(3) Korisnici su dužni izbjegavati aktivnosti koje bi mogle ugroziti sigurnost njihovih računala i informacijskog sustava Instituta.

Članak 28.

Pristup bežičnoj mreži moguće je jedino kao rješenje za privremene potrebe/posebne prigode (npr. u slučaju organizacije skupova ili događanja).

XI. ZAPORKA

Članak 29.

(1) Svi zaposlenici Instituta koji u svome radu koriste računala dužni su pridržavati se pravila korištenja zaporki, a administrator Instituta dužan je tehnički ugraditi zaporku u sve sustave koji to omogućavaju.

(2) Minimalna dužina zaporke mora imati osam znakova. Za zaporku se ne smiju koristiti riječi iz rječnika, niti imena bliskih osoba, ljubimaca, datuma i sl. U zaporci treba izmiješati mala i velika slova s brojevima.

(3) Korisnici su odgovorni za svoju zaporku i ni u kom je slučaju ne smiju otkriti čak ni administrator Instituta. Korisnik je odgovoran za tajnost svoje zaporke te mora naći način da je sakrije.

(4) Korisnici koji se ne pridržavaju navedenih pravila ugrožavaju sigurnost IS te će se protiv njih postupiti sukladno članku 25. stavak 3. ovog Pravilnika.

Članak 30.

Na računalima koja spadaju u zonu visokog rizika, administrator Instituta dužan je konfigurirati sustav na taj način da se korisnički račun zaključa nakon tri neuspjela pokušaja prijave.

XII. PRAVILO ČISTOG STOLA I ČISTOG EKRANA

Članak 31.

(1) Pravilom "čistog stola i čistog ekrana" Institut štiti osjetljive informacije o zaposlenicima, intelektualnom vlasništvu i/ili drugim fizičkim ili pravnim osobama s kojima Institut surađuje.

(2) Pravila se odnose na sve zaposlenike, a šteta koja nastane nepoštivanjem pravila - odgovornost je zaposlenika.
Pravila su sljedeća:

- zaposlenici moraju osigurati da su svi osjetljivi/povjerljivi tiskani ili elektronički podaci zaštićeni na kraju dana i kada očekuju dulje izbivanje,
- računala moraju biti zaključana kada se s njih izbiva,

- računala se moraju ugasiti na kraju radnog dana (u koliko je moguće, isključiti iz sklope i/ili direktno iz struje),
- sve povjerljive i osjetljive informacije moraju se ukloniti sa stola i zaključati kada se stol napušta bez nadzora i na kraju radnog dana,
- ključevi koji se koriste za pristup povjerljivim i osjetljivim informacijama ne smiju se držati na stolu koji nije pod nadzorom,
- prijenosna računala i svi prijenosni uređaji za pohranu podataka moraju se zaključati (u ladičar, ormar ili drugo),
- zaporke se ne smiju držati na samoljepljivim listićima na ili ispod računala odnosno na pristupačnom mjestu,
- tiskani materijali koji sadrže povjerljive ili osjetljive informacije moraju se smjesta preuzeti s pisača.

XIII. ANTIVIRUSNA ZAŠTITA I ZAŠTITA OD SPAMA

Članak 31.

Antivirusna zaštita podrazumijeva korištenje programa za zaštitu od virusa, ali i uzdržavanje korisnika od radnji koje ugrožavaju sigurnost IS.

Članak 32.

Zaštita od virusa je obavezna, a provode je pružatelji informatičkih usluga nadležni za pojedini dio sustava, i to na:

- poslužiteljima elektroničke pošte - ovlašteni CARNet sistem inženjeri,
- na internim poslužiteljima Instituta - administrator Instituta ili CARNet sistem inženjeri,
- svakom osobnom računalu korisnika - administrator Instituta.

Članak 33.

(1) Administrator Instituta dužan je instalirati antivirusne programe na sva korisnička računala i namjestiti ih tako da se izmjene u bazi virusa automatski propagiraju sa središnje instalacije ili s vanjskog poslužitelja bez aktivnog sudjelovanja korisnika.

(2) Korisnici ne smiju samovoljno isključiti antivirusnu zaštitu na svom računalu.

Članak 34.

(1) Administratori poslužitelja elektroničke pošte dužni su postaviti poslužitelje tako da se prilikom primanja poruka konzultira baze podataka koje sadrže popise poslužitelja koji su otvoreni za odašiljanje te baza sa adresama poznatih "spamera". Pošta koja dolazi s tako pronađenih adresa neće se primate.

(2) Administrator Instituta koji provodi zaštitu od virusa nije dužan čuvati elektronske poruke korisnika zaražene virusom ili spam poruke.

XIV. RJEŠAVANJE SIGURNOSNIH INCIDENATA

Članak 35.

(1) Svaki zaposlenik, poslovni partner ili suradnik Instituta dužan je prijavljivati sigurnosne incidente, poput usporenog rada servisa, nemogućnosti pristupa, gubitka ili neovlaštene izmjene podataka, pojave virusa itd.

(2) Administrator Instituta treba izraditi i održavati kontakt listu osoba kojima se prijavljuju problemi u radu mreže, mrežnih servisa i mrežne opreme te obrazac za prijavu incidenta.

(3) Svaki incident se dokumentira, a uz obrazac za prijavu incidenta, dokumentacija sadrži i obrazac sa opisom incidenta i poduzetih mjera pri rješavanju problema.

Članak 36.

(1) Administrator Instituta dužan je pratiti korisničke procese, a u slučaju sumnje da se računalo koristi na nedozvoljeni način, može izlistati sav sadržaj korisničkog direktorija.

(2) Daljnju istragu administrator Instituta ili osoba koju je ovlastio ravnatelj Instituta može se provesti samo uz suglasnost ravnatelja Instituta, uz poštivanje sljedećih pravila:

- istragu provodi ovlaštena osoba, uz prisustvo svjedoka kako bi se omogućilo svjedočenje o poduzetim radnjama,
- obvezno pravilo istrage je da se IS sačuva u zatečenom stanju odnosno da se ne učine izmjene koje bi otežale ili onemogućile dijagnosticiranje,
- najprije se napravi kopija zatečenog stanja po mogućnosti na takav način da se ne izmijene atributi datoteka,
- dokumentira se svaka radnja tako da se ponavljanjem zabilježenih akcija može rekonstruirati tijek istrage.

Članak 37.

(1) Izvještaj o sigurnosnom incidentu sastavlja ovlaštena osoba, smatra se povjerljivim dokumentom, sprema na sigurno mjesto i čuva 10 godina.

(2) Izvještaj iz stavka 1. ovog članka može poslužiti za statističke obrade kojima je cilj ustanoviti najčešće propuste radi njihova sprečavanja ili ponavljanja incidenta.

(3) U slučaju da je uzrok incidenta nastao radnjom korisnika, izvještaj iz stavka 1. ovog članka može se koristiti i kao dokazni materijal u eventualnim radnim i/ili sudskim procesima.

(4) Ravnatelj Instituta i administrator Instituta može korisniku odgovornom za sigurnosni oduzeti računalnu opremu na određeni broj dana (5,10 ili 30 dana) i/ ili ograničiti pristup na računalu.

(5) Slijedom pravila CARNeta, Institut je obvezan poduzimati sankcije prema korisnicima - sudionicima u računalnim incidentima zbog činjenice da CARNet može ograničiti ili uskratiti

pristup CARNet mreži Institutu, a u slučaju težih prekršaja, povrede zakona, CARNet ima pravo prekršitelja prijaviti nadležnim organima.

XVI. ZAVRŠNE ODREDBE

Članak 38.

(1) Izmjene i dopune ovog Pravilnika donese se na istovjetan način na koji je donesen ovaj Pravilnik.

(2) Ovaj Pravilnik objavit će se na oglasnim pločama Poljoprivrednog instituta Osijek, a stupa na snagu osmog (8) dana od dana objave.

Prof. dr. sc. Vlado Guberac
Predsjednik Upravnog vijeća
Poljoprivrednog instituta Osijek

Ovaj Pravilnik objavljen je na oglasnim pločama Instituta dana 21. 12. 2021. godine a stupio je na snagu dana 30. 12. 2021. godine.

Nakon stupanja na snagu, ovaj Pravilnik će se objaviti na mrežnoj stranici Instituta https://www.poljinos.hr/ .

Poljoprivredni institut Osijek
Ravnatelj
Prof. dr. sc. Zvonimir Zdunić, EMBA

PRILOG 1.

Izjava o prihvaćanju odredbi sigurnosne politike

Poljoprivredni institut Osijek posvećuje značajnu pažnju pitanjima informacijske sigurnosti i dužnost je svakog korisnika pridržavati se svih pravnih propisa koje reguliraju pitanja zaštite informacijskog sustava Instituta.

Korisnik prima na znanje i prihvaća sljedeće:

- da je odgovoran za sigurno, etično i zakonito korištenje informacijskog sustava i imovine Instituta;
- da će koristiti informacijski sustav na način koji neće onemogućavati ili umanjivati učinkovitost poslovnih procesa;
- da će koristiti isključivo programskih rješenja dobivenih od strane Instituta ili programskih rješenja otvorenog koda;
- da neće koristiti plug-in-ova koja nisu preporučena od strane informatičke podrška;
- da će mu se po isteku radnog odnosa na Institutu, u roku od 10 dana, ukinuti korisnički račun iz domene: @poljinos.hr ;
- da neće na vidljivom i lako dostupnom mjestu držati lozinke u pisanom obliku;
- da će prilikom napuštanja prostorije adekvatno zbrinuti službene dokumente za koje je odgovoran i zaključati računalo;
- da će se pridržavati svih sigurnosnih odredbi sigurnosne politike i mjera koje iz nje proizlaze;
- da je upoznat sa odredbama ***Pravilnika o sigurnosti informacijskog sustava*** i prihvaća njegove odredbe.

Ja, _____ (ime i prezime korisnika)

IZJAVLJUJEM

da sam suglasan sa svime gore navedenim i da ću snositi moralnu i materijalnu odgovornost ako povrijedim navedeni Pravilnik, ako omogućim trećim osobama da ih povrijede te ako nanesem štetu trećim osobama što potvrđujem svojim vlastoručnim potpisom

Datum,_____

Potpis korisnika

_____

PRILOG 2.

Izjava o čuvanju povjerljivih informacija

Poljoprivredni institute Osijek posvećuje značajnu pažnju pitanjima informacijske sigurnosti i dužnost je svake osobe koja pristupa opremi i programima Instituta da se pridržava svih pravnih propisa koji reguliraju pitanja zaštite informacijske imovine Instituta.

Izjava o čuvanju povjerljivih informacija primjenjuje se na osobe koji imaju pristup opremi i programima Instituta, a to su:

- administrator koji nije iz grupe pružatelja informatičkih usluga (članak 5. Pravilnika) koji pristupa instalaciji i podešavanju glavnog poslužitelja Instituta, instalaciji, podešavanju i nadzoru rada autorizacijskog sustava, web i mail poslužitelja i povezanih servisa Instituta,
- vanjski suradnici koji administriraju mrežnu i komunikacijsku opremu i poslužitelje ključnih servisa (članak 13. Pravilnika).

Osoba koja ima pristup opremi:

- odgovorna je za sigurno, etično i zakonito korištenje informacijskog sustava i imovine Instituta,
- koristiti informacijski sustav na način koji neće onemogućavati ili umanjivati učinkovitost poslovnih procesa,
- pridržavati se svih sigurnosnih odredbi sigurnosne politike i mjera koje iz nje proizlaze,
- obvezuje se na čuvanje profesionalnih i poslovnih tajni Instituta te mu se zabranjuje zloupotrebljavati prikupljene/obradene/korištene podatke te iste odavati/prosljeđivati drugima.
- dužna je upoznati se s *Pravilnikom o sigurnosti informacijskog sustava* i prihvaća njegov sadržaj

---

Ja, _____ (ime i prezime)

IZJAVLJUJEM

da sam suglasan sa svime gore navedenim i da ću snositi moralnu i materijalnu odgovornost ako povrijedim navedeni Pravilnik, ako omogućim trećim osobama da ih povrijede te ako nanesem štetu trećim osobama svojim vlastoručnim potpisom

Datum,_____

Potpis

_____