



ČAZMATRANS - NOVA d.o.o.

POLITIKA SIGURNOSTI KORIŠTENJA OSOBNIH RAČUNALA

ORGANIZACIJSKE MJERE ZAŠTITE OSOBNIH PODATAKA



SADRŽAJ

Članak 1.	3
OPSEG	3
Članak 2.	3
DEFINICIJE	3
Članak 3.	3
ULOGI I ODGOVORNOSTI	4
Članak 4.	4
Članak 5.	4
Članak 6.	4
Članak 7.	4
Članak 8.	4
ŽIVOTNI VIJEK RAČUNALA	5
Članak 9.	5
Članak 10.	5
Članak 11.	5
Članak 12.	5
Članak 13.	5
Članak 14.	5
UPORABA OSOBNIH RAČUNALA	6
Članak 15.	6
Članak 16.	6
Članak 17.	6
Članak 18.	6
Članak 19.	7
ZAPORKE	8
Članak 20.	8
ZAŠTITA OD ZLOĆUDNOG KODA	9
Članak 21.	9
DOSTUPNOST INFORMACIJA	9
Članak 22.	9
KORIŠTENJE PRIJENOSNIH RAČUNALA	9
Članak 23.	9



Članak 24.	9
Članak 25.	10
OSIGURANJE PRIMJENE	10
Članak 26.	10



ČAZMATRANS - NOVA društvo s ograničenom odgovornošću za prijevoze i usluge iz Čazme, M.Novačića 10, OIB:04767584912, skupno zastupano po članovima uprave Damiru Pavloviću, Robertu Šimleši, Berislavu Saraji (u daljnjem tekstu: Poslodavac/ Voditelj obrade) u skladu s člankom 5. i člankom 32. Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (dalje u tekstu: Opća uredba o zaštiti podataka)

donosi sljedeću

POLITIKU O SIGURNOM KORIŠTENJU OSOBNIH RAČUNALA

SVRHA POLITIKE

Članak 1.

Svrha politike je propisati primjeren način postupanja djelatnika s osobnim računalima.

Osobna računala su imovina trgovačkog društva (voditelja obrade) na kojima se mogu nalaziti osobni podaci i povjerljive informacije.

Primjerenim načinom postupanja smanjuje se mogućnost pojave nepredviđenih stanja koja mogu dovesti do prekida u radu i neovlaštenog otkrivanja podataka.

Primjereno korištenje računala osigurava čuvanje povjerljivosti informacija, sprječavanje curenja informacija te osiguranje dostupnosti informacija.

OPSEG

Članak 2.

Ovog se pravilnika obvezatno se moraju pridržavati svi djelatnici voditelja obrade koji se u svom radu koriste osobnim računalima u vlasništvu ovog voditelja obrade.

DEFINICIJE

Članak 3.

Izrazi korišteni u ovom Pravilniku imaju sljedeće značenje:

Korisničko računalo: pojedino računalo informacijskog sustava koje se koristi za obradu, pohranu ili prijenos podataka;



Informacijska sigurnost je stanje povjerljivosti, cjelovitosti i raspoloživosti podatka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda.

Povjerljivost: obilježje informacije da nije učinjena dostupnom ili otkrivena neovlaštenim osobama, entitetima ili procesima.

Raspoloživost: svojstvo podatka ili procesa koje omogućuje pristup i uporabljivost tog podatka ili procesa ovlaštenom korisniku, onda kada je to potrebno;

Zloćudni kôd: programski kôd koji učitavanjem u uređaj bez svjesnog pristanka korisnika čini neku štetu (primjerice računalni virusi, crvi, trojanski konji i slično)

ULOGE I ODGOVORNOSTI

Članak 4.

Za postupanje djelatnika u skladu s ovim pravilnikom odgovorne su ovlaštene osobe društva.

Članak 5.

Ovlaštena osoba za zastupanje društva koordinira procese koji osiguravaju implementaciju zaštitnih mjera na osobna računala kojim se djelatnici trgovačkog društva koriste za obavljanje svakodnevnih radnih zadataka.

Ovlaštena osoba za zastupanje odgovorna je za rješavanje mogućih incidenata proizašlih iz neprimjerenog korištenja osobnih računala.

Članak 6.

Osoba koju trgovačko društvo kao takvu imenuje (odgovoran je za nadzor, edukaciju i koordinaciju provedbe mjera ove Politike.

Članak 7.

Osobe na rukovodećem položaju dužne su provoditi i nadzirati provođenje ovom politikom propisanih mjera u domeni svojih nadležnosti.

Članak 8.

Svi djelatnici i vanjski suradnici koji koriste osobna računala u vlasništvu t.d. odgovorni su za primjereno korištenje osobnih računala u svom radu, te su dužni su postupati sukladno ovoj politici.



ŽIVOTNI VIJEK RAČUNALA

Članak 9.

Sve instalacije i podešenja osobnih računala obavlja se isključivo uz odobrenje ovlaštene osobe za zastupanje društva.

Ovlaštena osoba društva propisuje tehničke i radne karakteristike koje trebaju zadovoljiti osobna računala, te je dozvoljena nabava samo računala koji zadovoljavaju navedene karakteristike.

Članak 10.

Djelatnik svojim potpisom na Zadužnici za informatičku opremu potvrđuje preuzimanje osobnog računala te postaje odgovoran za profesionalno, etično i zakonito korištenje istog.

Članak 11.

Tehničke zahvate na osobnim računalima (promjena konfiguracije, zamjena pojedinih dijelova opreme) smiju obavljati samo za to ovlaštene osobe voditelja obrade ili ovlašteni serviseri uz nadzor djelatnika uz pisani nalog.

Korisnicima osobnih računala je zabranjeno obavljati tehničke zahvate iz prethodnog stavka ovoga članka.

Članak 12.

Trgovačko društvo vodi ažurne evidencije o osobnim računalima i njihovim perifernim uređajima.

Ova evidencija minimalno sadrži:

- Inventarni broj računala/periferne opreme
- Tip opreme (računalo, pisač, skener i sl)
- Korisnika računala

Svako premještanje računala ili njihovih perifernih uređaja s jedne lokacije na drugu odobrava, izvodi i evidentira ovlaštena osoba voditelja obrade.

Članak 13.

Po prestanku radnog odnosa, djelatnik je dužan vratiti osobno računalo i razdužiti sredstva rada.

Članak 14.

Zastarjela računala mogu se zamijeniti ili staviti izvan upotrebe samo od strane ovlaštene osobe voditelja obrade.



Rashodovanje računala i njihovo zbrinjavanje provodi se u skladu s Zakonom o elektroničkom otpadu.

Prije davanja računala u rashod provodi se brisanje podataka na diskovima računala.

UPORABA OSOBNIH RAČUNALA

Članak 15.

Voditelj obrade zadržava pravo nadzora nad načinom korištenja osobnih računala, kao i pravo procjene prihvatljivog korištenja informatičke opreme. Voditelj obrade će sankcionirati neprihvatljive oblike korištenja osobnih računala sukladno težini neprihvatljivog korištenja. Djelatnici su dužni upozoriti na svaki oblik neprihvatljivog ponašanja s osobnih računala.

Neprihvatljivim korištenjem osobnih računala smatra se svako korištenje osobnih računala na način koji bi doveo do povrede važećih zakona, propisa, pravila ili etičkih normi, te svako korištenje informatičke opreme na način koji može izazvati materijalnu ili reputacijsku štetu za voditelja obrade.

Povreda odredbi vezanih uz informatičku opremu ove politike također može rezultirati privremenim ili trajnim oduzimanjem prava korištenja osobnih računala.

Članak 16.

Osobna računala se smiju koristiti isključivo u poslovne potrebe, sa svrhom izvršavanja radnih zadaća.

Članak 17.

Djelatnici ne smiju samostalno instalirati softver na osobna računala.

Članak 18.

Svi djelatnici trebaju biti svjesni sigurnosnih zahtjeva za zaštitu osobnih računala te osigurati njihovu primjerenu zaštitu ako ih ostavljaju bez nadzora (npr. za vrijeme sastanka, stanke za ručak i sl.). Svako udaljšavanje od radnog mjesta na lokaciju s koje se nema vizualni nadzor nad pristupom računalu i stolu jest napuštanje radnog mjesta.

Pri napuštanju svog radnog mjesta, svi djelatnici moraju primjereno zaštititi svoja računala.

Primjerena zaštita uključuje obvezatno zaključavanje zaslona računala (Windows tipka + L) ili odjavu djelatnika (engl. *log off*). Zaključavanje zaslona ili odjava djelatnika nije nužna ako se nakon izlaska ured zaključava. Preporučeno je zatvaranje svih otvorenih sesija (engl. *session*) nakon završetka rada, osim ako se mogu zaštititi odgovarajućim mehanizmom za blokiranje, te odjava s poslužitelja koji se koristio.



Sva računala moraju imati namješteni čuvar zaslona (engl. *screensaver*) sa zaporkom koji se aktivira nakon perioda neaktivnosti od 10 minuta.

Obvezatno je isključivanje računala nakon završetka radnog vremena.

Članak 19.

Korisnik je pri korištenju računala dužan pridržavati sljedećih pravila:

1. važne informacije moraju biti fizički nedostupne svim osobama koje im nemaju ovlašten pristup;
2. kada nije u blizini radnog mjesta korisnik mora onemogućiti pristup sadržaju računala;
3. za vrijeme odsutnosti s radnog mjesta potrebno je da korisnik računala zaključa računalno („lock“) ili da se odjaviti s računala („log off“);
4. na kraju radnog dana potrebno je da korisnik računala isključi računalno;
5. svi tiskani dokumenti koji sadrže osobne podatke potrebno je da su uklonjeni s radnog stola i zaključani u ormar/ladicu kada se ne koriste ili nisu pod nadzorom (za vrijeme odsutnosti s radnog mjesta i na kraju radnog dana) to uključuje i vanjske medije (npr. USB, CD, vanjski disk) kao i prijenosna računala, tablete i ostale uređaje na kojima su pohranjeni osobni podaci;
6. korisnička imena i/ili zaporke potrebno je da nisu ostavljeni na vidljivim i lako dostupnim mjestima (ispod tipkovnice, na monitoru, u nezaključanim ladicama i dr. - više niže u tekstu);
7. tiskani dokumenti koji sadrže osobne podatke potrebno je odmah po korištenju ukloniti uklonjeni s printera, skenera, telefaksa, fotokopirnog aparata i slično;
8. Elektronička pošta dio je svakodnevne komunikacije, poslovne i privatne, no njeno korištenje može ozbiljno ugroziti sigurnost informacijskog sustava. Da bi prijetnje informacijskom sustavu izazvane neprimjerenom uporabom elektroničke pošte sveli na minimum, potrebno je pridržavati se sljedećih pravila:



- elektroničku poštu ne smijete se koristiti za slanje uvredljivih, omalovažavajućih, seksualno uznemiravajućih i drugih poruka sličnog sadržaja;
- molimo da se ne šalju lančane poruke kojima se opterećuju mrežni resursi;
- svaka napisana poruka smatra se dokumentom. Poruke koje nisu poslane Vama osobno nije dozvoljeno proslijediti dalje bez odobrenja autora;
- svaku poruku koja sadrži privitak sumnjivog sadržaja potrebno je provjeriti antivirusnim programom;
- tvrtka ima pravo filtriranja poruka s namjerom da zaustavi neželjenu elektroničku poštu (eng. spam);
- nije dozvoljena upotreba e-mail adrese odnosno sandučića elektroničke pošte u privatne svrhe;
- tvrtka ima pravo pregleda i nadzora svih sandučića elektroničke pošte;
- poruke koje su dio poslovnog procesa nužno je arhivirati i čuvati propisani vremenski period;
- moli se da korisnik ne šalje masovne poruke, bez obzira na njihov sadržaj;

ZAPORKE

Članak 20.

Prilikom postavljanja zaporka ne preporuča se koristiti riječi iz rječnika.

Hakeri posjeduju zbirke suvislih riječi (riječi iz rječnika, imena, prezimena itd.). Izborom suvisle riječi lako se probije zaporka. Zaporku je bitno odabrati na taj način da je lako pamtljiva (ne pohranjivati je zapisanu) i da je teška za otkrivanje.

Korisnici su odgovorni za svoju zaporku i ne smiju istu otkrivati nikome, čak ni administratorima sustava.

Zaporka se ne smiju ostavljati na papirićima koji su zalijepljeni na ekran, ostavljeni na stolovima ili u ladici. Korisnik je odgovoran za tajnost svoje zaporka te mora naći način da je sakrije. Ukoliko korisnik zaboravi zaporku, administrator će mu omogućiti da unese novu.



Potrebno savjesno i odgovorno odnositi se prema svim osobnim podacima s kojima se dolazi u kontakt i voditi računa da se svi osobni podaci s kojima se raspolaže adekvatno zaštite.

ZAŠTITA OD ZLOĆUDNOG KODA

Članak 21.

Sva osobna računala voditelja obrade zaštićena su od zloćudnog koda za tu svrhu dedikiranim softverom renomiranoga proizvođača. Zaštita se realizira na nivou operativnog sustava. Zaštitu od zloćudnog koda zaštitu djelatnik ne smije isključiti niti promijeniti njezine parametre.

Djelatnik koji primijeti poruku softvera za zaštitu od zloćudnog koda o potencijalnoj zarazi ili sumnja na zarazu, mora isključiti računalo i prijaviti to u što kraćem roku ovlaštenoj osobi Voditelja obrade.

DOSTUPNOST INFORMACIJA

Članak 22.

Sve informacije koje se koriste u poslovnim procesima moraju se nalaziti u originalu na informacijskim sustavima Voditelja obrade.

Nije dozvoljeno pohranjivati informacije Voditelja obrade isključivo na osobnim računalima.

Voditelj obrade ne provodi sigurnosnu pohranu korisničkih podataka sa osobnih računala.

KORIŠTENJE PRIJENOSNIH RAČUNALA

Članak 23.

Sva pravila u ovoj Politici za navedena osobna računala vrijede i za prijenosna računala, ali zbog dodatnih rizika proizašlih iz činjenice da se ova vrsta osobnih računala može iznositi iz radnih prostora propisuju se dodatne mjere zaštite.

Članak 24.

Djelatnici imaju pravo iznositi prijenosno računalo i drugu prijenosnu opremu izvan prostora za koju postoji evidencija o zaduživanju.

Djelatnik je odgovoran za zaštitu prijenosnih računala i prijenosne opreme od krađe i neovlaštenog pristupa u svako vrijeme i na svakom mjestu. U vrijeme kad se prijenosna računala i prijenosna oprema ne koristi, ona mora biti primjereno zaštićena od krađe ili neovlaštenog pristupa.

Djelatnici moraju poduzeti sve mjere predostrožnosti kako bi smanjili vjerojatnost krađe prijenosnih računala. Djelatnici ne smiju ostavljati prijenosna računala bez nadzora na javnim ili lako dostupnim mjestima (zračne luke, restorani, konferencijske dvorane, sjedalo automobila,...).

U slučaju neželjenog događaja (krađe ili gubitka prijenosnog računala ili druge prijenosne opreme), isti se odmah mora prijaviti ovlaštenoj osobi Voditelja obrade i Službeniku za zaštitu podataka koji donosi odluku o daljnjim koracima.

Članak 25.

Tijekom rada na javnim mjestima i na mjestima na kojima postoji prijetnja da neovlaštena osoba dobije uvid u informacije pohranjene na prijenosnom računalu, djelatnik treba voditi računa o tome da spriječi promatranje svog rada.

Djelatnici trebaju biti svjesni rizika nezaštićene komunikacije na mreži. Korištenje bežične lokalne mreže (*Wireless LAN*) i *Bluetooth* komunikacijskog protokola u javnim prostorima (npr. zračne luke, hoteli, restorani...) treba biti svedeno na minimum.

OSIGURANJE PRIMJENE

Članak 26.

Primjereni načini korištenja informacijskog sustava propisani ovim dokumentom proizlaze iz postojećih dobrih praksi i trenutačnih zakonskih propisa u području sigurnosti informacija i zaštite osobnih podataka.

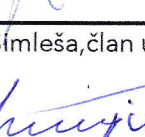
Ova politika preispituje se najmanje jednom godišnje o čemu se vodi pisana evidencija.

Datum donošenja: 19. prosinca 2024

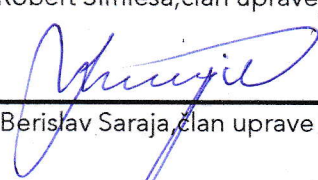
za ČAZMATRANS - NOVA d.o.o.



Damir Pavlović, član uprave



Robert Šimleša, član uprave



Berislav Saraja, član uprave

SLUŽBENIK ZA ZAŠTITU PODATAKA

Datum pripreme prijedloga:	prosinac 2024. godine
Službenik za zaštitu podataka:	Ines Krečak Data Protection Professional, CIPP/E E-mail: feralis@feralis.hr Mob.: +385(0)995639746

