



**LONJSKO
POLJE** Park prirode
Nature Park

Pravilnik

o računalnoj informacijskoj sigurnosti

Javna ustanova „Park prirode Lonjsko polje“

SADRŽAJ

1	Uvod.....	3
2	Opseg primjene pravilnika.....	3
3	Odgovornost.....	3
4	Administriranje računalne opreme.....	4
5	Zaporke i pristupni računi.....	5
6	Zaštita od zlonamjernog softvera.....	5
7	Fizička zaštita i sigurnost opreme.....	6
8	Neprekidnost poslovanja.....	6
9	Licenčna prava.....	6
10	Prekršaji i sankcije.....	6
11	Prijelazne i završne odredbe.....	7

Na temelju 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 (Opća uredba o zaštiti podataka), članka 21. stavka 2. podstavka 9. i članka 40. stavka 2. Statuta Javne ustanove Park prirode Lonjsko polje (Oznaka: I-547/14-DO-R od 26. rujna 2014.) ravnatelj Javne ustanove Park prirode Lonjsko polje donosi:

Pravilnik o računalnoj informacijskoj sigurnosti

1 Uvod

Članak 1.

Ovaj pravilnik donesen je sa svrhom da:

- Definira prihvatljive načine ponašanja u svezi korištenja računalnog informacijskog sustava Javne ustanove Park prirode Lonjsko polje (u daljnjem tekstu – Ustanova).
- Raspodjeli zadatke i odgovornosti nadležnih osoba.
- Zaštiti investiciju Ustanove u računalni informacijski sustav.
- Zaštiti informacije i podatke koji se u sustavu kreiraju, prenose, pohranjuju i obrađuju.
- Propiše sankcije u slučaju nepridržavanja odredbi ovog pravilnika.

Sastavni dio ovog pravilnika su i procedure

- Procedura upravljanja zaštitom od zlonamjernog softvera
- Procedura izrade sigurnosne kopije podataka

2 Opseg primjene pravilnika

Članak 2.

Ovaj pravilnik odnosi se na zaposlenike i vanjske suradnike (u daljnjem tekstu termin korisnik odnosit će se na sve osobe koje koriste informatički sustav Ustanove) kojima se dopušta uporaba računalnog informacijskog sustava Ustanove.

Pravilnik obuhvaća računalni informacijski sustav Ustanove i sve sadržaje koji se prenose, pohranjuju i obrađuju u tom sustavu, sadržaje pohranjene na svim osobnim računalima u vlasništvu Ustanove, kao i sve poslužitelje koji su u administrativnoj domeni ili vlasništvu Ustanove.

3 Odgovornost

Članak 3.

Za primjenu ovog Pravilnika i korištenje informatičke opreme u vlasništvu Ustanove najodgovorniji je ravnatelj Ustanove.

Poslove administriranja sustava obavlja informatička tvrtka (u daljnjem tekstu – administrator) s kojom je sklopljen ugovor za pružanje usluga IT administriranja.

Administrator je odgovoran za:

- administriranje i održavanje sigurnosti računalnog informacijskog sustava što uključuje materiju koju uređuje ovaj pravilnik, i sve pridružene procedure,
- pružanje odgovarajuće podrške korisnicima u ispunjavanju njihove obveze u odnosu na ovaj Pravilnik i pripadajuće procedure.

Svi korisnici obvezni su proučiti i primjenjivati ovaj Pravilnik. kao i njemu pridružene Procedure

Članak 4.

Ustanova štiti svoju računalnu opremu, sklopovlje, programsku podršku, podatke i dokumentaciju od zlouporabe, krađe, neovlaštene uporabe i upliva okoliša.

Za sigurnost računalnog informacijskog sustava Ustanove odgovorni su korisnici i administrator, svaki u svom dijelu odgovornosti propisane ovim Pravilnikom.

Povjerljivost i integritet podataka pohranjenih na računalnom informacijskom sustavu Ustanove moraju biti zaštićeni sustavom kontrole pristupa kako bi se osiguralo da samo ovlašteni korisnici imaju pristup potrebnim informacijama. Taj pristup treba biti ograničen na samo one informacijske sustave i mogućnosti koje su korisniku nužne za njegove poslovne aktivnosti.

Članak 5.

Administrator je odgovoran za sve instalacije, odspajanja, promjene i premještanje računalne opreme. Korisnici ne smiju samostalno poduzimati takve radnje (ovo se ne odnosi na prijenosna računala za koja je početnu konfiguraciju i priključenje u sustav obavio administrator sustava).

Članak 6.

Korisnici, glede informacijske sigurnosti, su obvezni pridržavati se slijedećih uputa:

- Mediji s podacima i programskom podrškom (diskete, diskovi, trake i ostali mediji) za vrijeme kada nisu u upotrebi, ne smiju biti izloženi na lako dostupnim mjestima neovlaštenim osobama;
- Mediji koji sadrže povjerljive i važne podatke trebaju biti čuvani u adekvatnim zaključanim kasama ili metalnim ormarima;
- Podatkovni mediji trebaju se čuvati podalje od nepovoljnih utjecaja okoliša kao što su toplina, direktno sunčevo svjetlo, vlaga i elektromagnetska polja i slično;
- Utjecaji okoliša kao što su dim, hrana, tekućine, previsoka ili preniska vlažnost, previsoke ili preniske temperature moraju se izbjegavati;
- Korisnici se trebaju s pažnjom odnositi prema povjerenoj im računalnoj opremi;
- Korisnik će se smatrati odgovornim za štete nastale na računalnoj opremi ako su nastale uslijed nepažnje ili nepravilne uporabe

4 Administriranje računalne opreme

Članak 7.

Računala moraju biti administrirana u skladu s pravilima struke, brinući istovremeno o funkcionalnosti i sigurnosti.

Za administraciju svih računala odgovoran je administrator sustava. On odgovara za instalaciju i konfiguraciju svih softvera na računalima.

Svako računalo zaštićeno je korisničkim imenom i lozinkom.

Članak 8.

Računala se moraju konfigurirati na taj 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.

Članak 9.

Posebnu pažnju administratori su dužni posvetiti opremi koja obavlja ključne funkcije ili sadrži vrijedne i povjerljive informacije koje treba štiti od neovlaštenog pristupa (npr. serveri, mrežna oprema i slično).

5 Zaporke i pristupni računici

Članak 10.

Zabranjuje se korištenje grupnih i univerzalnih pristupnih računa za pristup računalima i računalnim sustavima.

Svaka osoba obvezno mora pristupiti računalnom sustavu, računalima i informatičkim rješenjima (aplikacijama) Ustanove isključivo odobrenim pristupnim računom.

Članak 11.

Izuzetno, administrator sustava može na pismeno traženje ravnatelja Ustanove odobriti korisniku korištenje pristupnog računa druge osobe za pronalaženje i otklanjanje nepravilnosti rada sustava, o čemu treba sačiniti pisani dokument.

Nakon završetka radnji iz prethodnog stavka, obavezno treba promijeniti zaporku toga pristupnog računa.

Članak 12.

Administrator sustava obavezan je pohraniti sve administratorske zaporkke na mjesto koje odredi ravnatelj Ustanove.

Pohranjene zaporkke trebaju biti u svaka u zasebnoj zapečaćenoj kuverti, na kojoj treba pisati za koji je računalni sustav ili računalnu opremu, te datum kad je zadnji puta ažurirana.

Administrator sustava obavezan je redovito nakon svake promijene ažurirati pohranjene zaporkke.

6 Zaštita od zlonamjernog softvera

Članak 13.

Zaštita od zlonamjernog (*malware*) softvera (Računalni virusi, Računalni crvi, Trojanski konji, Logičke bombe, Rootkit, Spyware, Adware, Spamovi, Popupovi) je obavezna a provode ju:

- Davatelji informatičkih usluga na poslužiteljima elektroničke pošte
- Administrator na poslužiteljima Ustanove i osobnim računalima koja koriste zaposlenici Ustanove

Članak 14.

Osobe koje provode zaštitu od zlonamjernog softvera nisu dužne čuvati elektronske poruke korisnika zaražene zlonamjernim softverom.

Osobe koje provode zaštitu od zlonamjernog softvera dužne su instalirati protuvirusne programe na sva korisnička računala i namjestiti ih tako da se izmjene u zaštiti automatski propagiraju s središnje instalacije ili s vanjskog poslužitelja, bez aktivnog sudjelovanja korisnika.

Članak 15.

Korisnici ne smiju samovoljno isključiti zaštitu od zlonamjernog softvera na svome računalu. Ukoliko iz nekog razloga moraju privremeno zaustaviti program koji štiti od

zlonamjernog softvera, korisnici moraju zatražiti dozvolu od odgovornog zaposlenika Ustanove.

7 Fizička zaštita i sigurnost opreme

Članak 16.

U prostorijama Ustanove nalazi se informatička oprema (serveri, komunikacijska oprema, osobna računala) u vlasništvu Ustanove.

Administrator servera (ili druga osoba po odluci direktora) odgovorna je za održavanje ažurnog popisa sve računalne opreme.

8 Neprekidnost poslovanja

Članak 17.

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

Članak 18.

Procedura izrade rezervnih kopija propisana je u dokumentu Procedura izrade sigurnosne kopije podataka

9 Licenčna prava

Članak 19.

Obveza je Ustanove i svih njenih zaposlenika da poštuju zakone i propise o zaštiti intelektualnog vlasništva.

Ustanova je obvezno koristiti programsku podršku na temelju valjanih licenčnih prava.

Članak 20.

Ustanova programsku podršku i pripadajuću dokumentaciju koja nije u vlasništvu Ustanove nema pravo umnožavati i distribuirati bez dopuštenja proizvođača ili autora, osim za potrebe stvaranja sigurnosne kopije.

Članak 21.

Na računalima u vlasništvu Ustanove ne smije, se bez odobrenja direktora, koristiti programska podrška nabavljena privatno.

10 Prekršaji i sankcije

Članak 22.

Nedozvoljenim se smatra svako korištenje računala i/ili računalnog programa na način koji bi doveo do povrede važećih zakona, propisa ili etičkih normi, a mogao bi izazvati materijalnu ili nematerijalnu štetu za Ustanova.

Članak 23.

Lakšim oblicima nedozvoljenog korištenja računala i 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 neprimjerenog sadržaja (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 Ustanovi.

Članak 24.

Težim oblicima nedozvoljenog korištenja računala i opreme smatra se:

- Davanje podataka o vlastitom identitetu (korisničko ime, lozinka) drugima u Ustanovi i / ili izvan Ustanove
- Preuzimanje tuđeg identiteta (korištenje opreme s tuđim korisničkim računom, slanje elektroničke pošte pod tuđim imenom, kupovanje preko interneta 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 Ustanovi ili ne,
- Napad uskraćivanjem resursa na druga računala,
- Vrijeđanje i ponižavanje ljudi u internetskoj komunikaciji po vjerskoj, rasnoj, nacionalnoj ili nekoj drugoj pripadnosti,
- Korištenje mrežnih resursa Ustanove na način priključivanja vlastitih – privatnih računala na računalnu mrežu Ustanove.

Članak 25.

Svi korisnici računalnog sustava Ustanove dužni su pridržavati se odredbi ovog Pravilnika kao i svih drugih internih dokumenata / odluka koje reguliraju korištenje računalnog sustava i informatičke opreme.

Kršenje odredbi ovog Pravilnika i pripadnih procedura može korisnika izložiti opozivu prava uporabe računalnog sustava Ustanove, te pokretanju stegovnog postupka sve do prestanka ugovora o radu iz razloga uvjetovanog iskrivljenim ponašanjem radnika ili prestanka drugih primjenjivih ugovora.

Članak 26.

Sankcija za učinjenu povredu odnosno korištenje računalnog informacijskog sustava Ustanove protivno odredbama ovog Pravilnika ovisit će o vrsti i veličini prekršaja, zatim da li je prekršajem uzrokovana pravna, materijalna ili kakva druga šteta, te radi li se o prvom ili ponovljenom prekršaju.

Sankcije donosi ravnatelj Ustanove.

11 Prijelazne i završne odredbe

Članak 27.

Ovaj Pravilnik, zajedno sa pripadajućim procedurama, stupa na snagu prvog dana od dana objave na oglasnoj ploči Ustanove.

Prilagodni period za potpunu primjenu ovog Pravilnika i pripadajućih procedura traje šest (6) mjeseci od dana stupanja na snagu.



Ravnatelj

Ivor Stanivuković

Krapje, 20.05.2019.

KLASA:003-05/19-01/1

URBROJ:2176-144-02/01-19-1

Pravilnik o računalnoj informacijskoj sigurnosti u Javnoj ustanovi Park prirode Lonjsko polje objavljen je 20.05.2019. i stupio je na snagu 21.05.2019.