Temeljem članka 14. Statuta Parkovi d.d. Varaždin, Uprava-direktor dana 7.5.2018.godine donosi

SIGURNOSNU POLITIKU INFORMACIJSKOG SUSTAVA PARKOVA D.D.

1. **Potreba donošenja Sigurnosne politike**

Sigurnost informacijskih sustava sve je kompleksnija te je važno zaštititi informacijski sustav i osigurati uvjete za neprekinuto poslovanje i odvijanje svih procesa i odnosa zainteresiranih strana, odnosno uvjete za njihovo učinkovito i djelotvorno upravljanje, uz maksimalnu zaštitu podataka, posebno osobnih podataka. Ova Sigurnosna politika informacijskog sustava Parkova d.d. (u daljnjem tekstu: Sigurnosna politika) treba omogućiti uspostavu sigurnosti na svim kritičnim točkama informacijskog sustava, u bilo kojem segmentu sigurnosti.

Sigurnosna politika je dio sustava upravljanja sigurnošću informacijskih sustava u Parkovima d.d. (u daljnjem tekstu: Parkovi). To je skup pravila, smjernica i postupaka koja definiraju na koji način informacijski sustav učiniti sigurnim i kako zaštititi njegove tehnološke i informacijske vrijednosti. Ona govori korisnicima informacijskog sustava Parkova što smiju raditi, što ne smiju raditi, što moraju raditi i koja je njihova odgovornost.

Svakodnevnim razvojem tehnologija otkrivaju se i nove metode kojima je moguće ugroziti sustav. Stoga definiranje općenite sigurnosne politike za informacijske sustave nije moguće i jednom napisana politika mora se redovito pregledavati, mijenjati i nadopunjavati kada se za to ukaže potreba.

Dokumenti u elektroničkom obliku smatraju se službenim dokumentima na isti način kao i dokumenti na papiru, pa im treba osigurati čuvanje i pristup dopustiti samo ovlaštenim osobama.

2. **Cilj Sigurnosne politike**

Cilj Sigurnosne politike je zaštitili vrijednosti informacijskog sustava, uključuju i opremu, programsku podršku i podatke, i osigurati tri jedinstvena svojstva informacija:
- povjerljivost (tajnost)
- integritet
- dostupnost.

Uloga Sigurnosne politike je definirati prihvatljive i neprihvatljive načine ponašanja, jasno raspodijeliti zadatke i odgovornosti te propisati sankcije u slučaju njihova nepridržavanja.

3. **Reference i međunarodni standardi**

Reference i međunarodni standardi korišteni za izradu Sigurnosne politike su ISO 27001 i Opća uredba za zaštitu osobnih podataka (GDPR).

4. **Resursi informacijskog sustava Parkova**

Pravila koja definira Sigurnosna politika vrijede za:
- svu informatičku i komunikacijsku opremu koja se nalazi u prostorijama Parkova i priključena je u mrežu Parkova, na sav instalirani software i na sve mrežne servise
- administratore informacijskih sustava
- unutarnje korisnike, u koje spadaju: zaposlenici
- vanjske korisnike, u koje spadaju: konzultanti, auditori, revizije i inspekcije, korisnike sa pristupom informatičkoj tehnologiji (IT tehnologija), fizičkim komponentama (hardware), programskoj podršci (software), servisima (serverska tehnologija) i podacima Parkova.

Oblici komunikacije na koju se Sigurnosna politika odnosi su i: fax, e-mail, telefon, pregled internet stranica, internet marketing, društvene mreže i slično.

Prilikom zapošljavanja nove djelatnike treba upoznati s pravilima propisanim Sigurnosnom politikom.
Prilikom angažiranja novih vanjskih korisnika i administratora iste treba upoznati s pravilima propisanim Sigurnosnom politikom.

Odgovornost svakog korisnika i administratora je znati i pridržavati se smjernica iz ove Sigurnosne politike, a time i provoditi svoje aktivnosti u skladu sa njima.

Uprava-direktor je odgovoran za komunikaciju i primjenu Sigurnosne politike kroz pojedine odjele i službe Parkova.

5. **Organizacija upravljanja sigurnošću**

Ljudi koji se u radu koriste računalima dijele se na:
- unutarnje korisnike
- vanjske korisnike
- administratore.

6. **Unutarnji korisnici**

Unutarnji korisnici su osobe koje se u svom radu služe računalima, proizvode dokumente ili unose podatke, ali nisu odgovorni za instalaciju i konfiguraciju softwarea, niti za ispravan i neprekidan rad računala i mreže.

Unutarnji korisnik ima pravo uporabe odobrenih resursa, što se evidentira njihovim zaduženjem, osim za opće resurse koji su svima raspoloživi.

Unutarnji korisnici su dužni:
- pridržavati se pravila prihvatljivog korištenja, što znači da ne smiju koristiti računala za djelatnosti koje nisu u skladu sa važećim zakonima, etičkim normama i pravilima lokalne sigurnosne politike
- izabrati kvalitetne zaporke i povremeno ih mijenjati
- prijavljivati sigurnosne incidente kako bi problemi što prije nestali
- korisnici koji proizvode podatke i dokumente odgovorni su i za njihovo čuvanje i izradu sigurnosnih kopija te njihovo čuvanje.

Glavni korisnik:
Parkovi koriste aplikacije za obradu podataka. Radi poboljšanja sigurnosti za svaki od tih programa imenuje se glavni korisnik. Glavnog korisnika prema potrebi mijenja osoba koja mu je zamjena prema Organizacijskom ustrojstvu Parkova.

Zaposlenici koji unose podatke odgovorni su za njihovu vjerodostojnost, dok je glavni korisnik odgovaran za ispravnost podataka, za provjeru ispravnosti i sigurnosti aplikacije, za dodjelu dozvola za pristup podacima i za mjere sprečavanja izmjene podataka od neautoriziranih osoba.

Specijalist za sigurnost prema nalogu glavnog korisnika ili Uprave-direktora kontaktira proizvođača aplikacije i dogovara isporuku novih verzija, traži ugradnju sigurnosnih mehanizama itd.

7. **Vanjski korisnici**

Davateljima informatičkih usluga smatraju se profesionalni vanjski suradnici koji brinu o radu: računala, komunikacijske opreme, aplikacija i mreže. Oni su zaduženi za ispravnost i neprekidnost rada informacijskog sustava.

Davatelji informatičkih usluga osiguravaju automatsku pohranu (backup) važnih informacija sukladno ugovorima koji su s njima sklopljeni.

Davatelji usluga dužni su u svome radu poštivati privatnost korisnika i povjerljivost informacija s kojima pri obavljanju posla dolaze u dodir, a posebno osobnih podataka. Na poštivanje tih pravila obvezuju se potpisivanjem Izjave o upoznatosti i povjerljivosti.

Povremeno se osobama iz vanjskih tvrtki ili ustanova mora dopustiti pristup opremi, radi servisiranja, održavanja, podrške, obuke, zajedničkog poslovanja, konzultacija itd.

Parkovi u ugovore s vanjskim tvrtkama ugrađuju odredbe kojima obavezuju poslovne partnere na poštivanje sigurnosnih pravila.

Ako u sigurnu zonu radi potrebe posla ulaze osobe koje za to nemaju ovlasti, mora im se osigurati pratnja.

8. **Administratori**

Davatelji usluga dužni su administrirati računala i mrežnu opremu u skladu s pravilima struke, brinući istovremeno o funkcionalnosti i sigurnosti.

Podaci o administratorima smatraju se sastavnim dijelovima ugovora s davateljima usluga. Davatelj usluga dužan je bez odlaganja Parkovima prijaviti svaku izmjenu administratora i to pismeno i prije nastupa izmjene a administratori su dužni potpisati Izjavu o upoznatosti i povjerljivosti.

Posebnu pažnju administratori su dužni posvetiti onoj opremi preko koje se obavljaju ključne funkcije ili koja sadrži vrijedne i povjerljive informacije koje treba štiti od neovlaštenog pristupa.

Administratori su dužni prijaviti sve sigurnosne incidente Specijalistu za sigurnost bez odlaganja te pomoći pri istrazi i uklanjanju problema.

9. **Specijalist za sigurnost**

Brigu za organizaciju i provođenje sigurnosnih mjera navedenih u Sigurnosnoj politici vodi Specijalist za sigurnost imenovan od strane Uprave-direktora, a to uključuje:
- brigu za fizičku sigurnost sustava
- izradu pravilnika
- nadzor rada mreže i servisa
- izdavanje odobrenja za priključenje računala na mrežu
- organiziranje obrazovanja korisnika i administratora
- komunikacija s Upravom
- sudjelovanje u donošenju odluka o nabavi dijelova informacijskog sustava Parkova
- izrada i održavanje kontakt liste s brojevima telefona i e-mail adresama osoba kojima se prijavljuju sigurnosni incidenti
- i ostale poslove propisane Sigurnosnom politikom i pratećim radnim uputama.

10. **Upravljanje mrežom**

Za upravljanje mrežom, konfiguriranje mrežnih uređaja, dodjeljivanje adresa, kreiranje virtualnih LAN-ova i sl. zaduženi su vanjski suradnici.

Specijalist za sigurnost mora u svakom trenutku imati točan popis svih mrežnih priključaka i umreženih uređaja, uključujući i prijenosna računala, te izdaje odobrenje za priključenje računala na mrežu.

Ukoliko se podrži rad na daljinu (npr. kada se djelatnicima dopušta da sa kućnog računala ažuriraju podatke), bit će potreban poseban pravilnik kojeg će se morati poznavati i pridržavati ga se svi koji tako rade. Povjerljivi podaci na udaljenom računalu moraju biti jednako sigurni kao da se računalo nalazi u zgradi ustanove.

Za spajanje na mrežu gostujućih računala, koja donose sa sobom vanjski suradnici, predavači, poslovni partneri, serviseri i slično, zbog opasnosti od širenja virusa ili namjernih nedopuštenih radnji (poput presretanja mrežnog prometa, prikupljanja informacija itd.) ne smije se dozvoliti da oni po svom nahođenju priključuju računala na mrežu Parkova.

11. **Instalacija i licenciranje softwarea**

Korištenje ilegalnog softwarea predstavlja povredu autorskog prava i intelektualnog vlasništva. Korisnik koji ima potrebu za nekim programom mora se obratiti Specijalistu za sigurnost i zatražiti, uz obrazloženje, nabavu i instalaciju softwarea.

Svi korisnici obvezni su poštivati autorska prava i prava intelektualnog vlasništva.

12. **Fizička sigurnost i briga o opremi**

Fizičkom zaštitom i brigom o opremi želi se spriječiti neovlašteni pristup, ometanje poslovnih prostorija i nepotreban pristup korisnika osjetljivoj opremi te osigurati zaštita opreme od nepovoljnih utjecaja, sigurnost instalacija i održavanje opreme.

Da bi se osigurala fizička sigurnost implementirane su slijedeće točke sigurnosti:

- definirano je i dokumentirano tko je ovlašten pristupiti pojedinim dijelovima sustava
- kontrolnim mehanizmima spriječeni su potencijalni pokušaji neovlaštenog pristupa
- ulazi u prostorije su jasno naznačeni i osigurani
- svi kontrolni mehanizmi su periodički pregledavani kako bi se na vrijeme uočili nedostaci ili pokušaji neovlaštenog pristupa.

13. **Sigurne zone**

Dijelovi sustava na kojima se obavljaju najvažnije funkcije neophodne za funkcioniranje informacijskog sustava ili koji sadrže povjerljive informacije su sigurne zone u koje je ulaz dozvoljen samo ovlaštenim osobama.

Zaštićeni prostori su prostori u kojima je server i sustav videonadzora te arhiva.

14. **Prihvatiljivo korištenje**

Korištenje informacijskog sustava u vidu fizičkih komponenti (hardware), programske podrške (software), servisa (serverska tehnologija) i podataka Parkova namijenjeno je aktivnostima koje su potpora službenom poslovanju Parkova.

Ukoliko je korisnik nesiguran da li je ono što čini u skladu s prihvatljivim korištenjem, on/ona mora zatražiti od nadređene ili odgovorne osobe odnosno Specijalista za sigurnost smjernice za daljnje postupanje.

15. **Neprihvatljivo korištenje**

Neprihvatljivim korištenjem se smatra svako korištenje informacijskog sustava Parkova na način koji bi doveo do povrede zakona, propisa ili etičkih normi, koji je u suprotnosti s Sigurnosnom politikom i koji bi mogao izazvati materijalnu ili nematerijalnu štetu za Parkove i osobe čije osobne podatke Parkovi posjeduju.

Strogo se zabranjuje provoditi aktivnosti kao što su:

- ugrožavanje sigurnosti osobnih podataka koji se nalaze u zbirkama koje posjeduju Parkovi
- provođenje ilegalnih i nezakonitih radnji korištenjem informatičkim sustavom Parkova
- korištenje Interneta za potrebe nelegalnih radnji kao što su prevare i piratstvo, ali i objavljivanje kleveta i tajnih podataka tvrtke te podataka vezanih uz djelatnike, partnere ili klijente
- namjerno poduzimanje radnji koje uzrokuju uzaludno trošenje vremena zaposlenika te mrežnih resursa tj. IT infrastrukture kao što je sabotaža u vidu povećanog prometa ili općenito ometanje rada mrežne infrastrukture
- korištenje mreže na takav način da ometa korištenje drugim korisnicima, na primjer preopterećivanje pristupnih linija ili preklopne opreme
- uporaba tuđeg korisničkog računa
- davanje na uporabu svojeg korisničkog računa drugim osobama
- širenje virusa, trojanaca, crva i ostalog zloćudnog softwarea
- lažno predstavljanje kroz uporabu mrežnih usluga i servisa
- uporaba resursa ili podataka koji su dani na privatnu uporabu drugim osobama
- stavljanje informacija Parkova na javnu uporabu putem bez suglasnosti Parkova
- uporaba resursa izvan Parkova ili na način koji korisniku nije odobren
- uporaba mrežnih usluga i servisa koji su zaštićeni lozinkom ili pisanim upozorenjem vlasnika
- uporaba mrežnih usluga i servisa mimo pravila njihove uporabe
- korumpiranje ili uništavanje podataka drugih korisnika
- ometanje drugih korisnika u radu
- provaljivanje na računala koristeći sigurnosne propuste u softwareu
- masovna distribucija pojedinačnih poruka
- uporaba korisničkog računa u komercijalne svrhe
- distribuiranje ili publiciranje informacija koje su suprotne opće prihvaćenim moralnim normama ili narušavaju ugled ili privatnost pojedinca

- korištenje informatičkog sustava Parkova za lažne, pogrdne, uvredljive, nepristojne i pornografske svrhe, diskriminaciju bilo koje vrste, prijeteće, uznemirujuće ili nasilno ponašanje, promicanje političkih stavova i sklonosti, širenje mržnje i rasizma
- davanje netočnih ili zastarjelih podataka u svrhu ostvarivanja korisničkih prava
- priključivanje bilo kojeg uređaja, programa i/ili servisa na računalo i/ili mrežu bez isključive dozvole
- korištenje informatičkog sustava Parkova za kreiranje, pohranu, kopiranje, distribuciju, prijenos ili razmjenu ilegalnih kopija bilo kojeg materijala zaštićenog autorskim pravima
- kreiranje i distribucija sadržaja koji nagrđuju percepciju i ugled Parkova, direktora i zaposlenika
- korištenje informatičkog sustava Parkova za igrice, klađenja i slične aktivnosti
- povreda privatnosti drugih korisnika.

16. **Osobna upotreba**

Parkovi prepoznaju i dozvoljavaju postojanje povremene upotrebe informatičkog sustava Parkova za osobne potrebe zaposlenika, pri čemu oni sami moraju procijeniti i odlučiti o nužnosti i razumnosti takve upotrebe. Međutim, bilo koja osobna upotreba resursa Parkova izričito isključuje:
- kršenje bilo kojeg od uvjeta ove Sigurnosne politike
- umanjivanje radne efektivnosti i negativnog utjecaja na izvršavanje radnih zadataka
- izravno ili neizravno kompromitiranje sigurnosti, rada ili integriteta resursa u vlasništvu Parkova, informacija ili usluga informacijske tehnologije
- uzrokovanje osjetnog povećanja troškova IT usluga koje plaćaju Parkovi.

Prihvatljiva osobna upotreba informatičkog sustava Parkova može se smatrati ona koja je:
- kratka i nije česta
- ne ometa rad radnika, njegovih radnih kolega i općenito rad sustava
- ne kompromitira sigurnost Parkova i ne ugrožava kontinuitet sustava
- ne utječe na pefrormanse informacijskog sustava Parkova
- ne povećava troškove Parkova
- ne krši zakone
- u skladu s Etičkih kodeksom Parkova.

17. **Čuvanje poslovno vezanih datoteka i podataka**

Od zaposlenika se očekuje da poslovno vezane datoteke i podatke pohranjuju na službenim računalima, lokalnoj mreži ili dijeljenim zajedničkim mrežnim pogonima.

Pohrana privatnih multimedijalnih datoteka i zapisa (glazba, video snimke, fotografije i sl.) kao i izvršnih datoteka (igre, programi i sl.) na lokalnoj mreži i/ili dijeljenim zajedničkim mrežnim pogonima je izričito zabranjena.

Zaposlenici su odgovorni za sigurnost poslovno vezanih datoteka i podataka koji su pohranjeni lokalno na računalu i/ili na prijenosnim uređajima.

18. **Ekološka osvještenost**

Parkovi potiču ekološki odgovorno korištenje računala i IT tehnologije što uključuje upotrebu energetski učinkovitih računala i perifernih uređaja, kao i smanjenje potrošnje energetskih resursa.

Zaposlenicima se preporučuje da doprinesu ekološki odgovornom korištenju računala na slijedeće načine:
- pregledavanjem i ispravljanjem dokumenata na zaslonu/ekranu računala
- korištenjem obostranog ispisa i kopiranja dokumenata
- korištenjem i prosljeđivanjem elektroničke verzije dokumenta umjesto ispisane kad god je to moguće
- korištenjem e-pošte umjesto telefaksa
- gašenjem računala i perifernih uređaja kada nisu u upotrebi
- korištenjem značajki za upravljanje energijom na prijenosnim računalima.

19. **Sigurnost opreme**

Specijalist za sigurnost je dužan voditi popis sve računalne opreme, s opisom ugrađenih komponenti, inventarnim brojevima i slično.

Za fizičku sigurnost opreme odgovoran je Uprava-direktor. On odgovornost za grupe uređaja ili pojedine uređaje prenosi na druge zaposlene, koji potpisuju dokument kojim potvrđuju da su preuzeli opremu.

Čuvarska služba provjerava da li oprema koja se iznosi ima potrebne prateće dokumente, izdatnice, radne naloge za popravak i td.

20. **Osiguranje neprekidnosti poslovanja**

Kako bi se u slučaju nezgoda (poput kvarova na sklopovlju, požara, ili ljudskih grešaka) podaci sačuvali, potrebno je redovito izrađivati rezervne kopije svih vrijednih informacija, uključujući i konfiguraciju softwarea.

Preporučuje se čuvati sigurnosne kopije na različitim mjestima, po mogućnosti u vatrootpornim ormarima.

Povremeno se provjerava upotrebljivost rezervnih kopija podataka te izvode vježbe oporavka sustava. Vježbe se ne izvode na produkcijskim računalima, već na rezervnoj opremi (koju bi trebalo osigurati zaposlenicima zaduženim za te poslove).

21. **Nadzor nad informacijskim sustavima**

Parkovi zadržavaju pravo nadzora nad instaliranim softwareom i podacima koji su pohranjeni na računalima te nad načinom korištenja računala i informacijskog sustava Parkova.

Nadzor se smije provoditi radi:
- osiguranja integriteta, povjerljivosti i dostupnosti informacija i resursa
- provođenja istrage u slučaju sumnje da se dogodio sigurnosni incident
- provjere da li su informacijski sustavi i njihovo korištenje usklađeni sa zahtjevima Sigurnosne politike.

Nadzor smiju obavljati samo Specijalist za sigurnost i osobe koje Parkovi za to ovlaste. Pri provođenju nadzora ovlaštene osobe dužne su poštivati privatnost i osobnost korisnika i njihovih podataka. U slučajevima kada je korisnik prekršio pravila Sigurnosne politike ne može se više osigurati povjerljivost informacija otkrivenih u istrazi, pa se one mogu koristiti u stegovnom ili sudskom postupku, u skladu s pozitivnim propisima Hrvatske.

22. **Provođenje**

Korisnici su dužni pomoći osobama zaduženim za nadzor informacijskih sustavi te im pružiti sve potrebne informacije i omogućiti im pristup prostorijama i opremi radi provođenja nadzora.

Isto vrijedi i za administratore računala i pojedinih servisa, koji su dužni specijalistu za sigurnost pomagati pri istrazi.

Pristup uključuje:
- pristup na razini korisnika ili sustava svoj računalnoj opremi
- pristup svakoj informaciji, u elektroničkom ili tiskanom obliku, koja je proizvedena ili spremljena na opremi Parkova, ili oprema Parkova služi za njezin prijenos
- pristup radnom prostoru (uredu, sigurnoj zoni itd.).

23. **Nepridržavanje**

Kršenje pravila ove Sigurnosne politike može rezultirati gubitkom prava pristupa mreži i/ili pristupa računalu i/ili perifernom uređaju, kao i disciplinskim postupkom i/ili kaznenim progonom i/ili privatnom tužbom a za vanjske korisnike raskidom ugovornog odnosa i poslovne suradnje i naknadom štete prouzročene Parkovima i trećim stranama.

24. **Izvješće o kršenju pravila Sigurnosne politike**

Ukoliko dođe do kršenja pravila ove politike, direktor, zaposleniku nadređena osoba i ovlaštena osoba će biti službeno obaviješteni.

25. **Praktična primjena sigurnosne politike**

Kako bi se sigurnosna politika mogla što uspješnije primijeniti, nužno je održavati popis informatičkih i komunikacijskih uređaja s pripadajućim operacijskim sustavima i instaliranim aplikacijama te održavati skicu mreže.

26. **Vlasništvo, privatnost i povjerljivost**

Korisnici moraju biti svjesni da su sve podatke, dokumente ili poruke koje su stvorene, poslane ili primljene pomoću resursa Parkova isključivo vlasništvo Parkova. Kao rezultat toga isti ne mogu očekivati privatnost pri korištenju resursa Parrkova.

Tajnost elektroničke komunikacije ne može uvijek biti osigurana. Ona može biti kompromitirana zbog primjenjivosti zakona ili politike, nenamjernom distribucijom ili zbog neadekvatnosti postojećih tehnologija za zaštitu od neovlaštenog pristupa. Stoga se zaposlenici upućuju na povećani oprez kada se koriste bilo kojom vrstom elektroničke komunikacije.

27. **Sigurnost opreme i informacija**

Korisnici koji identificiraju ili primijete stvaran ili potencijalan sigurnosni problem o tome moraju odmah obavijestiti Specijalista za sigurnost au njegovom odsustvu nadređenu osobu.

Zaposlenici ni pod kojim okolnostima ne smiju odavati informacije o svojim korisničkim računima i lozinkama, niti dozvoliti bilo kojoj drugoj osobi korištenje istih.

Korisnici u pravilu moraju smatrati sve podatke u mreži Parkova kao povjerljive i spriječiti bilo kakav neovlašteni pristup tim podacima.

28. **Dokumenti u prilogu**

Prateći dokumenti koji su sastavni dio Sigurnosne politike Parkova su:
Uputa o administraciji korisničkih računa – RU-27.01
Uputa o rukovanju zaporkama – RU-27.02
Uputa o korištenju elektronicke pošte – RU-27.03
Uputa o pravilnom korištenju Interneta i društvenih medija -RU-27.04
Uputa o antivirusnoj zaštiti – RU-27.05
Uputa o upravljanju prijenosnim medijima -RU-27.06
Uputa o videonadzoru – RU-27.07
Uputa o izradi sigurnosnih kopija – RU-27.08
Uputa o upravljanju poslovnim kontinuitetom i rješavanju sigurnosnih incidenata – RU-27.09
Uputa o klasifikaciji informacija – RU-27.10
Uputa o korištenju informacijskih sustava Parkova za vanjske korisnike – RU-27.11
Uputa o korištenju prijenosnih racunala, tableta i mobitela – RU-27.12
Uputa o fizičkoj zaštiti informacijskog sustava – RU-27.13
Uputa o sigurnosti i ljudskim resursima – 27.14
Uputa o internoj dostavnoj službi – 27.15
Upravljanje rizicima sigurnosti informacija – DP-54.03
Pravilnik o postupanju u zaštiti osobnih podataka

Svi korisnici su dužni pridržavati se svih pratećih dokumenata koje su primjenjivi na njihov djelokrug rada.

29. **Obavijest o Sigurnosnoj politici**

Svi zaposlenici će biti obaviješteni o ovoj Sigurnosnoj politici od strane nadređene osobe.

Svaki zaposlenik potpisuje Izjavu o upoznatosti i povjerljivosti (OB-27.01) koja se čuva u personalnom dosjeu zaposlenika.

Svi vanjski suradnici u smislu ove Sigurnosne politike biti će obaviješteni o ovoj Sigurnosnoh politici prilikom sklapanja ugovora, odnosno nastupom okolnosti kada dođu u doticaj s informacijskim sustavom Parkova te potpisuju Izjavu o upoznatosti i povjerljivosti (OB-27.01).

30. **Završne odredbe**

Društvo kontinuirano radi na podizanju svijesti zaposlenika i ostalih korisnika o sigurnosti informacijskog sustava Parkova.

Provedbom Sigurnosne politike osigurava se sigurnost sustava od neovlaštenog pristupa te se smanjuje rizik od moguće štete koja bi nastala neovlaštenim pristupom informacijskom sustavu.

Sigurnosna politika stupa na snagu i počinje se primjenjivati 8 dana nakon objave.

Parkovi zadržavaju pravo izmjene i ispravaka ove Sigurnosne politike ukoliko će to okolnosti zahtijevati.

Uprava-direktor:
mr.sc. Alen Runac