

Nadzorni odbor KJKP "Park" d.o.o. Sarajevo

Broj P-02-5248-10-p

Dana, 26.11.2025. godine

Na osnovu člana 43. Prečišćenog teksta Statuta KJKP „Park“ d.o.o. Sarajevo, broj: P-2802-3/21, od 31.08.2021. godine i člana 19. Poslovnika o radu Nadzornog odbora, broj: P-4384-2-1 od 15.12.2021. godine, na 45. redovnoj sjednici održanoj dana 26.11.2025. godine, Nadzorni odbor KJKP „Park“ d.o.o. Sarajevo, donosi sljedeću

ODLUKU

Član 1.

Donosi se Pravilnik o prihvatljivom korištenju informacionog sistema u KJKP „Park“ d.o.o. Sarajevo.

Član 2.

Ova odluka stupa na snagu danom donošenja.



**PREDSJEDNIK
NADZORNOG ODBORA**

Dostavljeno:

1. Nadzorni odbor,
2. Uprava,
3. SOP,
4. Web,
5. Oglasna ploča,
6. Sekretar,
7. Vijeće zaposlenika,
8. Sindikalna organizacija,
9. SKP,
10. a/a.

PRAVILNIK

o prihvatljivom korištenju informacionog sistema u KJKP"Park" doo Sarajevo

Pravilnik je usklađen sa Zakonima i
važećim propisima za navedenu oblast

Rukovodilac SKP /

↓

Sarajevo, novembar 2025. godine

Tel. Centrala: +387 33 560 560;
Direktor: +387 33 560 570.
Fax: +387 33 560 561;
E-mail: info@park.ba;
www.park.ba

Općinski sud u Sarajevu
Broj sudskog registra UF/I-2558/05
Porezni broj: 01071306;
Matični broj: 20379383;
Matični registracioni broj: 1-566

NLB Banka 1322602019095668;
UniCredit bank d.d 3386902212020028;
Turkish Ziraat bank Bosnia d.d. Sarajevo
1860001022085047

Na osnovu člana 43. Prečišćenog teksta Statuta KJKP „Park“ doo Sarajevo, broj P-2802-3/21 od 31.08.2021 godine, Nadzorni odbor na svojoj sjednici održanoj dana 26.11.2025. godine donosi :

PRAVILNIK

o prihvatljivom korištenju informacionog sistema u KJKP”Park” doo Sarajevo

Član 1.

Pravilnikom o prihvatljivom korištenju informacionog sistema (u daljem tekstu: „Pravilnik”) regulišu se uslovi prihvatljivog internet pristupa zaposlenika KJKP „Park” d.o.o. Sarajevo (u daljem tekstu: „Preduzeće”). Pravilnikom se ne uređuju zahtjevi, standardi i procedure za razvoj i implementaciju internet servisa.

Član 2.

Internet predstavlja izvor informacija koji može biti koristan za svakog zaposlenika u Preduzeću. U slučaju da efikasnost zaposlenika može biti unaprijeđena upotrebom interneta, politika Preduzeća je da se takvim zaposlenicima obezbijedi internet pristup, te da im se omogući obuka i profesionalno usavršavanje kako bi zaposlenik mogao optimalno iskoristiti mogućnosti interneta.

Član 3.

Korištenje interneta u preduzeću dozvoljeno je isključivo za službene potrebe i ograničeno je na stranice i podatke koji mogu biti korisni za izvršavanje radnih zadataka i obaveza, a u skladu s radnim mjestom i opisom posla zaposlenika. Sva ograničenja vezana za korištenje interneta uvode se iz sigurnosnih razloga, kao i radi omogućavanja nesmetanih primarnih poslovnih komunikacija.

Član 4.

Zaposlenici koji koriste računar imat će svoj elektronički identitet. Elektronički identitet uključuje šifru – lozinku za pristup računaru, službenu e-mail adresu s korisničkim imenom i šifrom, kao i pravo pristupa uslugama na mreži. Korisničko ime i šifra moraju biti jedinstveni za svakog zaposlenika – korisnika. Zabranjeno je ustupati svoj elektronički identitet drugima na korištenje, kao i koristiti tuđi identitet.

Konkretno, nije dozvoljeno davati svoje korisničko ime i šifru kolegama kako bi dobili pristup internetu. Korisnik je odgovoran za sve što je učinjeno s njegovim identitetom. Svoju šifru ne smije otkriti ni službenim osobama.

Član 5.

Kao dio čuvanja identiteta, korisnik je dužan koristiti složene šifre koje nije lako pogoditi te ih mijenjati svaka tri mjeseca. Šifra se ne smije držati zapisana u blizini računara, jer bi se time ukinula njezina tajnost. Što je šifra duža, to ju je teže otkriti i trebalo bi da se sastoji od najmanje 8 znakova, sadržavati kombinaciju velikih i malih slova, brojeva i specijalnih znakova, npr. n3To%iROv+.

Član 6.

Zaposleniku nisu dozvoljene sljedeće aktivnosti prilikom korištenja i upotrebe službenog računara:

- korištenje računarske opreme za privatne potrebe,
- unošenje i korištenje privatne računarske opreme te spajanje iste na sistem mreže,
- samostalno instaliranje i deinstaliranje postojećih programa,
- neovlašteni pristup drugim računarima i njihovim podacima,
- korištenje računarskih igara i pristup internet stranicama neprikladnog sadržaja,
- omogućavanje pristupa računarskoj opremi neovlaštenim osobama,
- samoinicijativno instaliranje bilo kakvog softvera, dodataka, programa ili alata na službene uređaje,
- neovlašteno otvaranje, rastavljanje ili fizičko mijenjanje informatičke opreme,
- pristupanje sumnjivim i neprovjerenim web stranicama,
- korištenje interneta za lične potrebe koje mogu ometati rad ili ugroziti sigurnost sistema (npr. streaming, igrice, društvene mreže, skidanje filmova, muzike i sl.),
- preuzimanje neovlaštenog softvera, sadržaja ili dokumenata koji mogu ugroziti sigurnost sistema.

Član 7.

U slučaju kvara, neispravnosti ili sumnjivog ponašanja uređaja, korisnik je dužan odmah obavijestiti sturčno lice zaduženo za održavanje informacionog sistema radi provjere i intervencije. Stručno lice zaduženo za održavanje informacionog sistema vrši instalaciju softvera, dodataka, programa ili alata na službene uređaje uz provjeru kompatibilnosti, sigurnosti i licencne ispravnosti softverskih rješenja.

Član 8.

Zaposlenik ima sljedeće obaveze prilikom korištenja i upotrebe službenog računara:

- Svaki korisnik računarske opreme odgovoran je za podatke koji se nalaze na računaru kojim se koristi. U slučaju da više korisnika koristi jedan računar, rukovodilac službe odredit će koji će korisnik biti odgovoran za podatke na tom računaru.
- Korisnik računarske opreme dužan je sa svim elektronskim zapisima postupati savjesno, s pažnjom dobrog domaćina.
- Snimanje internih podataka vrši korisnik računara.

Član 9.

Zabranjeno je prikupljati informacije o drugim računarima, tražiti ranjivosti i iskorištavati ih kako bi se dobio pristup tuđim računarima i podacima (hakiranje). Korisnik koji na računaru ima spremljene programe i alate koji omogućuju traženje ranjivosti i njihovo iskorištavanje čini krivično djelo, prema članu 186. Krivičnog zakona FBiH.

Član 10.

Zaposlenik koji se ne pridržava pravila prihvatljivog korištenja računara, računarske opreme i upotrebe interneta, kao i pravila propisanih članovima 6., 7. i 8. ovog Pravilnika, može biti sankcionisan u skladu s Pravilnikom o disciplinskoj i materijalnoj odgovornosti zbog povrede radne obaveze.

Član 11.

Zaposleniku se odobrava korištenje službenog e-maila u preduzeću isključivo za službene potrebe. Cilj korištenja e-maila jeste ubrzanje poslovanja i komunikacije s korisnicima usluga.

Član 12.

Komunicirajući s ljudima na internetu, korisnik je dužan pridržavati se pravila lijepog ponašanja (netiquette). Nije dozvoljeno vrijeđanje i ponižavanje ljudi po vjerskoj, nacionalnoj, spolnoj, rasnoj ili bilo kojoj drugoj osnovi. Zabranjeno je distribuiranje materijala koji šire mržnju ili netoleranciju.

Korisnik ne smije slati spam poruke, poruke u kojima nešto oglašava, niti poruke koje sadrže veliku količinu podataka osobama koje takve informacije nisu tražile. Zabranjeno je slanje i prosljeđivanje lanaca sreće i sličnih elektronskih poruka putem e-maila.

Nedozvoljeno je korištenje bilo kakvih programa za razmjenu elektronskih poruka u eksternoj komunikaciji.

Član 13

Zaposlenik prilikom slanja e-mail pošte ima sljedeće dužnosti:

- Korisnik koji na svom računaru ima instaliran e-mail račun (account) mora dobro poznavati rad s programom za razmjenu elektronske pošte.
- Korisnik mora poznavati pravila *netiquette*-a (pravila pristojnosti na internetu).
- Obavezno je u poruku unositi predmet poruke („Subject“).
- Treba izbjegavati slanje velikih fajlova u privitku (attachmentu); prije slanja potrebno ih je zapakovati.
- U slučaju potrebe za slanjem više velikih fajlova, treba ih razdvojiti u posebne poruke (sa jasnom naznakom rednog broja poruke u „Subject“).
- Umjesto slanja Wordovih ili Excelovih dokumenata (čiji sadržaj primalac lako može promijeniti), te fajlove potrebno je prethodno pretvoriti u PDF format.
- Na kraju poruke potrebno je navesti osnovne kontakt podatke.
- Ukoliko korisnik prosljeđuje poruku koju je primio, ne smije mijenjati njen sadržaj.
- Ne koristiti VELIKA SLOVA niti boldirati cijelo tekst, osim tamo gdje je neophodno.

Član 14.

Zaposlenik prilikom prijema e-mail pošte ima sljedeće dužnosti:

- Prilikom prijema pošte, sva pošta pregledava se na postojanje virusa već na samom mail serveru, te na ulazu u našu mrežu. Ipak, stopostotna zaštita ne postoji i korisnik uvijek treba biti oprezan prilikom otvaranja primljene pošte.
- Sumnjive e-mail poruke potrebno je odmah brisati, bez otvaranja, kao i poruke kojima u rubrici „Subject“ (predmet) nije ništa napisano, a radi se o nepoznatom pošiljaocu.
- Poruke sa „Subjectom“ na engleskom ili nekom drugom stranom jeziku, po pravilu, treba odmah brisati.
- Poruke koje se zaprimaju na stranim jezicima, a od nepoznatog pošiljaoca, potrebno je odmah izbrisati, jer postoji mogućnost da sadrže viruse (spam).

Član 15.

Zaposleniku nisu dozvoljene sljedeće aktivnosti prilikom korištenja i upotrebe službene e-mail adrese:

- Korištenje službenog e-maila za privatne svrhe
- Slanje poruka koje sadrže osjetljive podatke bez predhodne enkripcije ili bez odobrenja
- Otvaranje sumnjivih e-mailova, linkova i priloga.

Član 16.

Stručno lice zaduženo za održavanje informacionog sistema treba omogućiti, iz oblasti informatike, sljedeće mjere zaštite:

- a) odgovarajuće mjere zaštite opreme na kojima se vrši obrada podataka
- b) posebnim mjerama zaštite podataka treba onemogućiti neovlašten pristup i njihovu obradu
- c) mjere zaštite podataka obavezno obuhvataju kontrolu pristupa prostorijama i opremi za obradu službenih podataka, zaštitu od uništenja i oštećenja podataka i drugo.

Član 17.

Stručno lice zaduženo za održavanje informacionog sistema, pri automatskoj obradi službenih podataka, treba osigurati mjere zaštite podataka i to:

- a) jedinstveno korisničko ime i lozinka
- b) automatsku izmjenu lozinke po utvrđenom vremenskom periodu, koji ne može biti duži od šest mjeseci
- c) korisničko ime i lozinka dozvoljavaju pristup samo onim dijelovima sistema potrebnim izvršiocu za izvršenje njegovih radnih zadataka
- d) automatsko odjavljivanje sa sistema po isteku određenog perioda neaktivnosti, ne dužeg od 15 minuta; za ponovno aktiviranje sistema potrebno je ponovo upisati korisničko ime i lozinku
- e) automatsku zabranu pristupa sistemu nakon tri neuspješna pokušaja prijavljivanja, uz automatsko upozorenje izvršiocu da potraži instrukciju od administratora baze podataka
- f) efikasnu i sigurnu antivirusnu zaštitu sistema, koja se stalno ažurira radi preventive od

nepoznatih ili neplaniranih opasnosti od novih virusa g) kompjuterska, programska i ostala neophodna oprema na elektroenergetsku mrežu priključuje se putem uređaja za neprekidno napajanje

U slučaju iz tačke e), stručno lice zaduženo za održavanje informacionog sistema odobrava daljnji pristup sistemu.

Član 18.

Stručni saradnik za radne odnose treba izvještavati stručno lice zaduženo za održavanje informacionog sistema o zaposlenju ili angažiranju svakog izvršioca s pravom pristupa informacionom sistemu, kako bi mu se dodijelili korisničko ime i lozinka, kao i po prestanku zaposlenja ili angažiranja, da bi se korisničko ime i lozinka izbrisali, odnosno zabranio daljnji pristup.

Navedeno izvještavanje vrši se i prilikom bilo koje druge promjene radnog statusa izvršioca, koja utiče na nivo ili obim pristupa bazi podataka.

Član 19.

Stručno lice zaduženo za održavanje informacionog sistema radi sigurnosti kopiranja i arhiviranja podataka, ima sljedeće dužnosti:

- a) vrši redovno snimanje sigurnosnih kopija ili arhiviranje podataka u sistemu, kako ne bi došlo do njihovog gubljenja ili uništenja
- b) provjerava upotrebljivost sigurnosnih kopija podataka, uz provjeru postupka povrata podataka pohranjenih na prenosivom informacionom mediju, tako da vraćeni podaci nakon izvršene provjere budu u cijelosti raspoloživi za upotrebu, bez gubitka informacija
- c) svaki primjerak kopije podataka, ukoliko je pohranjen na prenosivom informacionom mediju, mora biti označen brojem, vrstom, datumom pohranjivanja te imenom lica koje je pohranjivanje izvršilo.

Član 20.

Na službenim računarima i informatičkim sistemima smije se koristiti isključivo softver koji je:

- licenciran,
- prethodno odobren od strane stručnog lica zadužena za održavanje informacionog sistema i menadžmenta,
- instaliran od strane ovlaštenog stručnog lica zadužena za održavanje informacionog sistema ili uz njihovu asistenciju.

Član 21.

Zaposlicima nije dozvoljeno samoinicijativno instaliranje bilo kakvog softvera. uključujući:

- probne verzije, nekomercijalne alate ili besplatne aplikacije bez posebnog odobrenja menadžmenta ili odgovornih lica pisanim putem,

- softver preuzet sa interneta bez provjere sigurnosti i licence,
- igre, peer-to-peer aplikacije, download managere i slično.

Član 22.

Stručno lice zaduženo za održavanje informacionog sistema ovlašteno je da, uz poštivanje važećih zakonskih propisa i prava na privatnost, vrši nadzor nad:

- pristupom mrežnim i informacionim resursima,
- korištenjem službenih e-mail naloga,
- mrežnim saobraćajem,
- instalacijom i upotrebom softvera,
- logovima pristupa sistemima i osjetljivim podacima.

Član 23.

Pristup podacima pohranjenim u zbirka podataka dozvoljen je upotrebom dodijeljenog jedinstvenog korisničkog imena i propusnice. Zabranjeno je, na bilo koji način umnožavati baze informacionih medija koje sadrže podatke iz zbirki posebnih kategorija službenih podataka.

Član 24.

Svaki pristup informacionom sistemu za vođenje zbirki službenih podataka mora biti automatski zabilježen korisničkim imenom, datumom i vremenom prijave i odjave. Svaki pokušaj neovlaštenog pristupa sistemu mora se također automatski zabilježiti korisničkim imenom, datumom i vremenom, a ako je to moguće i mjestom s kojeg je takav pristup pokušan.

O takvim pokušajima stručno lice zaduženo za održavanje informacionog sistema obavještava upravu Preduzeća.

Član 25.

Za uredno provođenje mjera osiguranja, pohranjivanja i zaštite podataka odgovoran je stručno lice zaduženo za održavanje informacionog sistema.

Član 26.

Nadzor nad provedbom ovog Pravilnika vrši KJKP „Park“ d.o.o. Sarajevo. Sve firme i državne institucije koje na bilo koji način informatički sarađuju s KJKP „Park“ d.o.o. moraju biti upoznate sa sadržajem ovog Pravilnika i u korespondenciji elektronskim putem s KJKP „Park“ d.o.o. prihvatati njegove odredbe

Član 27.

- (1) Ovaj Pravilnik stupa na snagu osmog dana od dana objave na oglasnoj tabli KJKP "Park" d.o.o. Sarajevo.
- (2) O danu objavljivanja Pravilnika sačinjava se službena zabilješka koju ovjerava poslodavac.
- (3) Danom stupanja na snagu ovog Pravilnika, prestaje da važi Pravilnik o prihvatljivom korištenju informacionog sistema u KJKP „PARK“ d.o.o. Sarajevo, broj P-15-20-3/10 od 02.06.2010.g.



Predsjednik Nadzornog odbora

Broj: P-02-5248-10-p-1
Sarajevo, 26.11.2025. godine

Službena zabilješka

Pravilnik o prihvatljivom korištenju informacionog sistema u KJKP "Park" doo Sarajevo objavljen je na oglasnoj ploči Preduzeća dana 01.12.2025., a stupa na snagu osmog dana od dana objavljivanja, 12.09.2025. godine.



Pis i pečat ovlaštenog lica