Pravilnik o prihvatljivom korištenju informacionog sistema u KJKP"Park"d.o.o. je u skladu sa zakonom
Rukovodioc Službe za opšte,pravne poslove
Jasminka Dorić,dipl.pravnik

KJKP »Park» d.o.o. Sarajevo

PRAVILNIK O PRIHVATLJIVOM KORIŠTENJU INFORMACIONOG SISTEMA

April,2010.godine

Na osnovu člana 33.Statuta KJKP"Park"d.o.o. Sarajevo,Nadzorni odbor na svojoj 55.sjednici održanoj dana 02.06.2010.godine donio je slijedeći

PRAVILNIK O PRIHVATLJIVOM KORIŠTENJU INFORMACIONOG SISTEMA

Član 1.

Pravilnikom o prihvatljivom korištenju informacionog sistema (u daljem tekstu Pravilnik) regulišu se uvjeti prihvatljivog internet pristupa zaposlenika KJKP"Park"d.o.o.Sarajevo (u daljem tekstu preduzeća).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 obezbjedi internet pristup, te da se istim omogući obuka i profesionalno usavršavanje kako bi zaposlenik mogao optimalno iskoristiti mogućnosti interneta.

Član 3.

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

Član 4.

Zaposlenici koji koriste računar imat će svoj elektronički identitet.
Elektronički identitet uključuje zaporku-lozinku za pristup računaru, službenu e-mail adresu sa korisničkim imenom i zaporkom kao i pravo za pristup uslugama na mreži. Korisničko ime i zaporka moraju biti jedinstveni za svakog zaposlenika-korisnika.Zabranjeno je ustupati svoj elektronički identitet drugima na korištenje, kao i korištenje tuđeg identiteta.
Konkretno, nije dozvoljeno davati svoje korisničko ime i zaporku kolegama, kako bi dobili pristup internetu. Korisnik je odgovoran za sve što je počinjeno s njegovim identitetom. Svoju zaporku ne smije otkriti niti službenim osobama.

Član 5.

Kao dio čuvanja identiteta, korisnik je dužan koristiti složene zaporke koje nije lako pogoditi, te ih mijenjati svaka tri mjeseca. Zaporka se ne smije držati zapisana u blizini računra, jer bi se time ukinula njezina tajnost. Što je zaporka duža, to ju je teže otkriti, a najbolje se sastoje od mješavine velikih i malih slova,brojeva i posebnih znakova, npr. n3To%iR0v+.

Član 6.

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

- koristiti računarsku opremu za privatne potrebe
- unošenje i korištenje privatne računarske opreme i stavljanja iste u sistem mreže
- samostalno instaliranje i deinstaliranje postojećih programa
- neovlašteni pristup drugim računarima i njihovim podacima
- korištenje računarskih igara i Internet pristup stranicama neprikladnog sadržaja
- samostalno rastavljanje računarske opreme
- omogućavanje pristupa računarskoj opremi neovlaštenim osobama

Član 7.

Zaposlenik ima slijedeće obaveze prilikom korištenja i upotrebe službenog računara:

- Svaki korisnik računarske opreme je odgovoran za podatke koji se nalaze na računaru kojim se koristi. U slučaju da više korisnika koristi jedan računar, rukovodilac službe će odrediti koji će korisnik biti odgovoran za podatke na konkretnom računaru.
- Korisnik računarske opreme je dužan da sa svim elektronskim zapisima rukuje savjesno, s pažnjom dobrog domaćina.
- Rukovodilac svake službe je dužan da osigura permanentnu zaštitu svih podataka koji se nalaze na računarima u njegovoj službi.
- Snimanje internih podataka vrši korisnik računara.

Član 8.

Nije dozvoljeno 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 F BiH.

Član 9.

Zaposlenik koji se ne pridržava pravila prihvatljivog korištenja računara, računarske opreme i upotrebe interneta i pravila propisanim članom 6.,7. i 8.ovog Pravilnika,pored navedenog mogu biti sankcionisani prema Pravilniku o disciplinskoj i materijalnioj odgovornosti zbog povrede radne obaveze.

Član 10.

Stručni saradnik za informacione sisteme ima ovlaštenje i obavezu da sankcioniše korisnike koji se ne pridržavaju propisanih pravila, prvo opomenom (putem e-maila), sedmičnim isključenjem, te trajnim isključenjem. Za ove postupke,stručni saradnik za informacione sisteme mora prezentovati dokaz u vidu izvoda iz "log" fajla u kojem se prati kompletan internetski saobraćaj, i poslati ga prekršiocu ove zabrane i rukovodiocu Službe kojoj prekršioc pripada.

Član 11.

Zaposleniku se odobrava korištenje službenog e-mail-a u preduzeću isključivo za službene potrebe.
Cilj korištenja e-maila je ubrzanje poslovanja i komunikacije sa korisnicima usluga.
Svaki korisnik e-maila ima obavezu njegovog korištenja (prijema, slanja i prosljeđivanja poruka korisnicima koji nemaju kreiran e-mail račun).

Član 12.

Komunicirajuci s ljudima na internetu, korisnik je dužan pridržavati se pravila lijepog ponašanja(*netiquette*).Nije dozvoljeno vrijedanje i ponižavanje ljudi po vjerskoj, nacionalnoj, spolnoj, rasnoj ili nekoj drugoj osnovi. Nije dozvoljeno distribuiranje materijala koji širi mržnju, netrpeljivost, strahove, potiče na nasilje ili je uvredljiv.
Korisnik ne smije slati spam poruke, poruke u kojima nešto oglašava, poruke koje sadrže veliku količinu podataka osobama koje takve informacije nisu tražile.
Zabranjeno je slanje i proslijeđivanje lanaca sreće i slične elektronske pošte e-mailom.
Nedozvoljeno je korištenje bilo kakvih programa za razmjenu elektronskih poruka u eksternoj komunikaciji.

Član 13.

Zaposlenik prilikom slanja e-mail pošte ima slijedeće dužnosti:

- Korisnik koji na svom računaru ima instaliran e-mail račun (account) mora dobro poznavati rad sa 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 (attachment-u); prije slanja potrebno ih je zapakovati
- U slučaju potrebe za slanjem više velikih fajlova, treba ih razdvojiti u posebne poruke (sa jasnom naznakom broja poruke u subject-u)
- Umjesto slanja wordovih ili excelovih dokumenata (čiji sadržaj primalac lako može promijeniti), te fajlove je potrebno prethodno pretvoriti u pdf format.
- Na kraju poruke, potrbno je navesti osnovne kontakt podatke.
- Ukoliko korisnik prosljeđuje poruku koju je primio, ne smije mijenjajti njen sadržaj (može je kratiti i citirati ali naznačiti njenog autora);
- Ne koristiti VELIKA SLOVA niti boldirati cijeli tekst, osim tamo gdje je neophodno.

Član 14.

Zaposlenik prilikom prijema e-mail pošte ima slijedeće dužnosti:

- Prilikom prijema pošte, sva pošta je pregledana na postojanje virusa već na samom mail serveru, te na ulasku u našu mrežu. Ipak, stoprocentna zaštita ne postoji i korisnik uvijek treba biti oprezan prilikom otvaranja primljene pošte.
- Korisnik mora znati da li je njegov antivirusni program ažuran (antivirusna datoteka ne smije biti starija od sedam dana !)
- Radi sprječavanja automatskog otvaranja fajlova koji stižu uz e-mail (privitak – attachment), korisnik mora znati privremeno isključiti ovu zaštitu kako bi otvorio očekivanu poštu, te je poslije toga ponovo postaviti.
- Sumnjive e-mail poruke je potrebno odmah brisati, bez otvaranja, kao i poruke kojima u rubrici Subject (predmet) nije ništa napisano, a radi se o nepoznatom pošiljaocu. Poruke sa Subject-om na engleskom ili nekom drugom stranom jeziku po pravilu treba odmah brisati.
- Poruke koje se zaprimaju na stranim jezicima,a od nepoznatog pošiljaoca,potrebno ih je odmah izbrisati iz razloga što postoji mogućnost virusa (spam).

Član 15.

Prilikom postupanja sa elektronskom poštom svaki rukovodilac službe je dužan klasificirati vrstu elektronske pošte koja je primljena/poslana, po važnosti:

- trajna elektronska pošta – ovu poštu, neophodno je kopirati na poziciju **\My Documents\email** (odmah po prijemu pošte);
- Backup se mora uraditi jednom sedmično, pod imenom: email070203, gdje šest cifara predstavlja dan-mjesec-godinu kada je napravljen.
- operativna elektronska pošta – rok čuvanja 1 mjesec na HDD u samom programu za elektronsku poštu, bez potrebe pravljenja backupa; nakon ovog perioda poštu je potrebno izbrisati, te isprazniti 'kantu za smeće'.

Član 16.

Prilikom postupanja sa grafičkim podacima svaki rukovodilac službe je dužan klasificirati vrstu grafičkih dokumenata koji su u opticaju, po važnosti:

- trajni dokumenti (šeme, planovi, itd.) – sedmično pravljenje backupa
- operativni dokumenti – rok čuvanja 1 mjesec na HDD, bez potrebe pravljenja backupa.

Član 17.

Stručni saradnik za informacione sisteme treba omogućiti,iz oblasti informatike,slijedeće tehničke mjere zaštite:

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

Član 18.

Stručni saradnik za informacione sisteme pri automatskoj obradi službenih podataka treba da osigura tehničke mjere zaštite podatka i to:

a) jedinstveno korisničko ime i lozinku.
b) automatsku izmjenu lozinke po utvrđenom vremenskom periodu koji ne može biti duži od šest mjeseci;
c) korisničko ime i lozinka će dozvoljavati pristup samo do dijelova sistema potrebnih izvršiocu za izvršenje njegovih radnih zadataka;
d) automatsko odjavljivanje sa sistema po isteku određenog perioda neaktivnosti, ne duže od 15 minuta, a za ponovno aktiviranje sistema potrebno je nanovo upisati korisničko ime i lozinku;
e) automatsku zabranu pristupa sistemu nakon tri neuspješna pokušaja prijavljivanja na sistem i automatsko upozorenje izvršiocu da potraži instrukciju od administratora baze podataka;
f) efikasnu i sigurnu antivirusnu zaštitu sistema, koje će se stalno ažurirati radi preventive od nepoznate ili neplanirane opasnosti od novih virusa;
g) kompjuterska, programska i ostala neophodna oprema na elektorenergetsku mrežu se priključuje putem uređaja za neprekidno napajanje.

U slučaju iz tačke e) stručni saradnik za informacione sisteme odobrava daljnji pristup sistemu.

Član 19.

Stručni saradnik za radne odnose, treba da izvještava stručnog saradnika za informacione sisteme o zaposlenju ili angažiranju svakog izvršioca s pravom pristupa informacionom sistemu, kako bi 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 pristupu baze podataka.

Član 20.

Stručni saradnik za informacione sisteme,za sigurnost kopiranja i arhiviranja podataka ima slijedeće dužanosti:

a) vrši redovno snimanje sigurnosnih kopija ili arhiviranje podataka u sistemu, da ne bi došlo do njihovog gubljenja ili uništenja.
b) provjerava upotrebljivost sigurnosnih kopija zbirki uz provjeru postupka povrata zbirki pohranjenih na prenosivom informatičkom 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 informatičkom mediju, mora biti označen brojem, vrstom, datumom pohranjivanja, te imenom lica koje je pohranjivanje izvršilo.

Član 21.

Pristup podacima pohranjenim u zbirkama podataka dozvoljen je upotrebom dodijeljenog jedinstvenog korisničkog imena i propusnice,te je zabranjeno bez nadzora i odobrenja stručnog saradnika za informacione sisteme, na bilo koji način umnožavati baze informatičkih medija koja sadrže podatke iz zbirki posebnih kategorija službenih podataka.

Član 22.

Svaki pristup informacijskom sistemu za vođenje zbirki službenih podataka mora biti automatski zabilježen korisničkim imenom, datumom i vremenom prijave i odjave,te svaki pokušaj neovlaštenog pristupa sistemu mora se automatski zabilježiti korisničkim imenom, datumom i vremenom, ako je to moguće i mjestom s kojeg je takav pristup pokušan.
O takvim pokušajima stručni saradnik za informacione sisteme obavještava Upravu.

Član 23.

Za uredno provođenje mjera osiguranja, pohranjivanja i zaštite podataka odgovara stručni saradnik za informacione sisteme.

Član 24.

Razmjena podataka između KJKP"Park"-a i drugih državnih organa i firmi se vrši isključivo na univerzalnim formatima za razmjenu podataka (nikako na posljednjim verzijama odgovarajućih računarskih programa).

Član 25.

Nadzor nad provedbom ovog Pravilnika vrši KJKP"Park"d.o.o.Sarajevo.
Sve firme i državne institucije koje na bilo kakav način informatički sarađuju sa KJKP "Park"-om d.o.o moraju biti upoznate sa sadržajem ovog pravilnika i u korespodenciji elektronskim putem sa KJKP"Park"-om d.o.o. prihvatati njegove odredbe.

Član 26.

Izmjene i dopune ovog Pavilnika vrše se na način i po postupku utvrđenom za njegovo donošenje.

Član 27.

Ovaj pravilnik stupa na snagu osmog dana od dana objavljivanja na oglasnoj tabli preduzeća.

Predsjednik Nadzornog odbora
Mersa Kustura, dipl. pravnik

Broj JN: 15 20-3

Dana: