P R A V I L N I K o upravljanju sigurnosnim i poslovnim rizicima

I. OPĆE ODREDBE
Članak 1.

Ovim se Pravilnikom, a s ciljem zaštite, uređuju načini zaštite osobnih i drugih podataka, obveza čuvanja poslovne tajne Društva, pristup i korištenje računalnim sustavima, postupanje u slučaju sigurnosnih incidenata, te obveza povrata informacija.

Ovaj se Pravilnik, u smislu obveznosti svog sadržaja, primjenjuje na zaposlenike Društva (uključujući uz osnovu ugovora o radu, ugovore o djelu i autorske ugovore, studentske ugovore, te druge pravne oblike).

Ovaj se Pravilnik, u smislu obveznosti svog sadržaja vezano za sigurnu obradu osobnih podataka u skladu sa Općom uredbom o zaštiti podataka (GDPR) i Zakonom o provedbi opće uredbe o zaštiti podataka te općim aktima Društva primjenjuje i na Izvršitelje obrade (u smislu čl. 28 GDPR), te na sve pojedince koji imaju pristup osobnim podacima, te iste obrađuju po uputama, u ime Društva.

Ovaj Pravilnik propisuje načine korištenja informatičkih resursa društva. Cilj ovog Pravilnika je osigurati djelotvorno, efikasno, etično i zakonski primjereno korištenje resursa informacijskog sustava od strane svih zaposlenika i/ili vanjskih partnera društva koji koriste resurse informacijskog sustava Društva (u daljnjem tekstu: Korisnik/Korisnici).

II. OBVEZA ČUVANJA POSLOVNE TAJNE
Članak 2.

Ovim se Pravilnikom određuju podaci koji se u poslovanju Društva smatraju poslovnom tajnom, označavanje tajne, dužnost čuvanja tajnih podataka, ovlasti za priopćavanje tajne, zaštita i postupanje s tajnim podacima te druge okolnosti od interesa za čuvanje poslovne tajne.

Poslovnu tajnu predstavljaju podaci koji su određeni ovim Pravilnikom, a koji u suštini predstavljaju podatke zbog čijeg bi priopćavanja neovlaštenoj osobi, mogle nastupiti štetne posljedice za interese Društva.

Podatak u smislu ovog Pravilnika jest dokument, odnosno svaki napisani, umnoženi, nacrtani, slikovni, tiskani, snimljeni, fotografirani, magnetni, optički, elektronički ili bilo koji drugi zapis podatka, kao i prilozi, saznanje, mjera, postupak, predmet, usmeno priopćenje ili informacija koja s obzirom na svoj sadržaj ima važnost povjerljivosti i cjelovitosti za Društvo, a radi se o podacima koji su nastali u okviru djelatnosti Društva ili su s tom djelatnošću povezani.

Izraz "poslovne tajne" obuhvaća sve vrste podataka koji nisu opće poznati izvan Društva, te čije bi otkrivanje ili prenošenje moglo naštetiti gospodarskim interesima Društva kao što su, između ostalog:
- informacije o kupcima, marketinški poslovi, rezultati razvoja, softver, izumi, unapređenja, metode i dr., a koje se odnose na proizvode ili usluge koje Društvo, kupci ili kooperanti prodaju, odnosno rabe ili mogu prodavati, odnosno rabiti u budućnosti,
- informacije koje se odnose na poslovne odnose, aktivnosti i metode Društva, kupaca ili kooperanata,
- osobni podaci zaposlenika, klijenata i trećih osoba sukladno zakonskoj regulativi i uredbi GDPR,
- informacije o plaćama, troškovima, prihodima, organizaciji, popisima kupaca i modelima kalkulacija cijena,
- podaci iz ugovora koje Društvo zaključuje,
- podaci, ugovori i isprave koje poslovni partneri Društva i druge osobe označe kao poslovnu tajnu,
- financijski izvještaji, podaci o tekućem financijskom i materijalnom poslovanju Društva osim izvještaja koji prema posebnom propisu podliježu javnoj objavi,
- podaci o pristupu administrativnim sučeljima računalnih servisa,

- podaci koji se odnose na pristup bazama podataka i drugim resursima informatičke tehnologije (npr. passwordi),
- interni akti Društva kojima se uređuje unutarnji rad i poslovanje,
- podaci iz kadrovske evidencije zaposlenika, osim kada se dostavljaju nadležnim državnim tijelima i ustanovama, sukladno zakonu, ugovoru i sl.
- podaci koji sadrže ponude na natječaj ili dražbu – do završetka natječaja ili dražbe, sukladno zakonu,
- podaci koji su zakonom, drugim propisom ili općim aktom donesenim na temelju zakona, utvrđeni kao tajni podaci od posebnog gospodarskog značenja,
- drugi podaci koje direktor/odgovorna osoba društva, usmeno ili pismeno, utvrdi kao tajne jer bi objavljivanje tih podataka zbog njihove prirode i značenja moglo naštetiti poslovanju Društva, njegovim članovima ili poslovnim partnerima.

Članak 3.

Zaposlenik je obvezan:
- čuvati i ne otkrivati poslovne tajne trećoj osobi bez pisane dozvole Društva,
- pridržavati se naputaka (pismenih ili usmenih) Društva o poslovnim tajnama, kao što su npr. zahtjev da se određene informacije ne smiju iznositi iz prostora Društva ili da se mogu prenijeti samo određenim zaposlenicima Društva,
- u slučaju saznanja za bilo kakvo neovlašteno objavljivanje, kopiranje ili drugi način uporabe poslovnih tajni Društva, odmah obavijestiti Društvo i potpuno surađivati na zaštiti takve informacije.

Članak 4.

Zaposleniku se zabranjuje:
- iskorištavati (izravno ili neizravno) poslovne tajne Društva u druge svrhe, osim za izvršenje poslova za obavljanje kojih ima zaključen ugovor o radu s Društvom, u skladu sa dobivenim ovlastima,
- fotokopirati, digitalno kopirati ili drukčije umnožavati poslovne tajne Društva, osim ako to zahtjeva posao ugovoren s Društvom.

Članak 5.

Ne smatra se povredom čuvanja poslovne tajne priopćavanje podataka koji se smatraju poslovnom tajnom ako se to priopćavanje obavlja fizičkim osobama ili pravnim osobama kojima se takvi podaci mogu ili moraju priopćavati:
1) na temelju zakona i drugih propisa,

2) na temelju ovlasti koja proizlazi iz dužnosti koju obavljaju, položaja na kome se nalaze ili radnog mjesta na kojem su zaposleni.
Ne smatra se povredom čuvanja poslovne tajne priopćavanje podataka koji se smatraju poslovnom tajnom na sjednicama, ako je takvo priopćavanje nužno za obavljanje poslova.

Ovlaštena osoba koja na sjednici priopćava podatke koji se smatraju poslovnom tajnom, dužna je upozoriti nazočne da se ti podaci smatraju poslovnom tajnom, a nazočni su dužni ono što tom prilikom saznaju čuvati kao poslovnu tajnu.

III. UPRAVLJANJE OSOBNIM I DRUGIM PODACIMA

Članak 6.

Zaposlenik i svaka druga osoba na koju se odredbe Pravilnika odnose dužni su u upravljanju osobnim podacima u ime Društva postupati sukladno svrhama obrade, uputama Društva, relevantnim propisima, te isključivo u okviru ovlaštenja svog radnog mjesta i/ili ugovornih ovlaštenja.

Društvo i izvršitelji obrade u ime društva nastojati će osigurati što viši nivo zaštite osobnih podataka imajući u vidu odredbu članka 32. Opće uredbe o zaštiti podataka (GDPR).

IV. NAČELA SIGURNOSNE POLITIKE DRUŠTVA

Zaštita zapisa
Članak 7.

Svi važni zapisi u društvu moraju biti, razmjerno mogućnostima, zaštićeni od gubitka, uništenja i krivotvorenja.

Članak 8.

Troškovi primjene mjera sigurnosti moraju biti razmjerni s osjetljivošću i vrijednošću informacije koje se takvim mjerama štite.

Sprečavanje zloupotrebe resursa za obradu informacija
Članak 9.

Informacijski sustav i njegovi dijelovi mogu se koristiti samo za svrhe poslovnih procesa društva. Nije dopušteno koristiti dijelove informacijskog sustava na način koji vodi njihovu prekomjernom iskorištavanju. Takvo korištenje uključuje, između ostalog, i slanje masovne elektroničke pošte („mass mailing“, lanaca elektroničke pošte (SPAM), primanje elektroničke pošte koje nisu vezane za poslovnu svrhu (mailing liste, forumi...), prekomjerno korištenje Interneta, računalne igre ili stvaranje nepotrebnog mrežnog prometa na neki drugi način.
Zaposlenici su dužni koristiti informacijski sustav društva isključivo u poslovne svrhe, osim ako uprava Društva drukčije ne odredi.

Usklađenost sa sigurnosnim politikama i standardnima
Članak 10.

Voditelji ili druge ovlaštene osobe unutar svojih odjela u dogovoru s voditeljem IT odjela ili drugom ovlaštenom osobom moraju kontrolirati provođenje sigurnosnih politika i procedura definiranih u okviru područja primjene, kako bi se osigurala usklađenost sustava s implementiranom dokumentacijom sustava informacijske sigurnosti. Ukoliko tijekom kontrole voditelj odjela ili druga ovlaštena osoba uoči neku neusklađenost, mora u suradnji s voditeljem IT odjela ili drugom ovlaštenom osobom procijeniti da li je potrebno napraviti korektivnu radnju, te ukoliko je, izvršiti je i provjeriti da li je korektivna radnja postigla željeni učinak. Mora se sačuvati zapis o provedenoj korektivnoj radnji.
Provođenje kontrole mora se obavljati najmanje jednom godišnje. Plan provjere usklađenosti radi se u suradnji s voditeljem IT odjela ili drugom ovlaštenom osobom.

Pregledi sustava
Članak 11.

Svi testovi i pregledi koji uključuju provjere na radnim sustavima moraju se isplanirati kako bi se povećala učinkovitost pregleda, a smanjio utjecaj na normalno poslovanje.
Testovi i pregledi se moraju koordinirati te biti odobreni od voditelja IT odjela ili druge nadležne osobe Društva.
Svi resursi potrebni za pregled sustava moraju se identificirati prije samog pregleda, te moraju biti raspoloživi za sam pregled.
Sve provjere koje ne koriste "read-only" pristup podacima moraju se provoditi na testnim podacima, a testni podaci moraju biti anonimizirani kako u niti jednom trenutnu ne bi došlo do mogućnosti povrede internih ili zakonskih propisa o zaštiti podataka.
Svi softverski alati za pregled sustava, kao i rezultati pregleda, moraju biti zaštićeni od neovlaštenog pristupa.

Članak 12.

Uprava Društva donosi odluke, naputke i druge provedbene dokumente koji detaljnije uređuju pojedine odredbe upravljanja sigurnosti, načina korištenja i provedbe programa sigurnosti informacijskog sustava. Sustav sigurnosti mora se pregledavati od strane Uprave (ili osoba odobrenih od Uprave) barem jednom godišnje.
Uprava Društva (ili osoba odobrena od Uprave) daje nalog za provedbu mjera sigurnosti informacijskog sustava.
Uprava Društva treba pratiti razinu sigurnosti informacijskog sustava na način da bude upoznata sa odstupanjima od standarda propisanog sigurnosnom politikom, o svim težim prekršajima sigurnosne politike i o pojavi sigurnosnih incidenata. Uprava Društva može imenovati voditelja sigurnosti informacijskog sustava.

Voditelji pojedinih organizacijskih dijelova društva su odgovorni za provođenje mjera sigurnosti i pridržavanje sigurnosne politike i svih sigurnosnih pravilnika unutar organizacijskih cjelina za koje su nadležni.

Odgovornost za informacijsku imovinu
Članak 13.

Pod informacijskom imovinom se smatra svaki materijalni ili nematerijalni resurs informacijskog sustava ili organizacijske strukture Društva koji služi za prikupljanje, obradu, spremanje ili distribuciju informacija značajnih u poslovnom procesu.

Takvi resursi mogu biti podaci (uključujući osobne podatke), programski moduli, dokumentacija, ugovori, informatička oprema, dijelovi infrastrukture, pomoćne usluge i slično.

Podaci se smatraju naročito vrijednim oblikom informacijske imovine.

Svi korisnici provode sve mjere sigurnosti koje su u njihovoj nadležnosti, a koje su definirane ovim Pravilnikom i drugim općim aktima Društva.

Korisnik je svaki zaposlenik ili vanjski partner Društva koji ima pristup informacijskoj imovini Društva, sukladno svojoj ulozi u poslovnim procesima.

Ovlasti dodijeljene pojedinom korisniku ne smiju prelaziti ovlasti koje ta osoba obavlja u redovitom poslovnom procesu.

Rad s trećim osobama (partnerima)
Članak 14.

Društvo može ugovoriti obavljanje pojedinih usluga, te obrade podataka s trećim stranama. U takvim slučajevima treće strane moraju preuzeti obavezu primjerene skrbi sigurnosti informacijskog sustava i imovine Društva.

Pristup do resursa informacijskog sustava iz prethodnog članka, može biti omogućen samo sukladno ugovoru s trećim stranama. Ako suradnja s trećim stranama podrazumijeva i pristup informacijskom sustavu Društva, onda ugovor o poslovnoj suradnji s vanjskim partnerom mora uključivati i ugovor o povjerljivosti podataka.

Takav ugovor mora uključivati sve odredbe sigurnosne politike koje su relevantne za rad s vanjskim partnerima, te obavezu o ne-otkrivanju podataka.

Pristup trećih strana može biti odobren nakon prihvaćanja ugovora o suradnji.

Kadrovska pitanja i informatička sigurnost
Članak 15.

Voditelj/zaposlenik službe kadrovskih poslova ili druga ovlaštena osoba Društva je dužan pravovremeno dojaviti IT odjelu ili drugoj nadležnoj osobi podatke o prestanku radnog odnosa ili promjeni radnog mjesta Zaposlenika.

Zaposlenici IT odjela ili druge nadležne osobe su dužni oduzeti prava pristupa svim Korisnicima kojima prestaje radni/ugovorni odnos.

Unaprjeđenje svijesti zaposlenika o važnosti sigurnosnog programa je ključno za njegovu primjenu. Zaposlenici moraju biti upoznati s metodama zaštite i sigurnosnim mjerama. Program obuke se mora provoditi redovito u okviru redovitog programa edukacije (ili upućivanje zaposlenika na nove naputke) te mora obuhvaćati sve nove zaposlenike. Zaposlenici su dužni upoznati se s dokumentacijom i uputama koje opisuju mjere sigurnosti.

Minimalni zahtjevi za fizičku sigurnost računalnih resursa
Članak 16.

Fizički pristup računalnoj opremi i uređajima određen je sukladno potrebi za njihovim korištenjem. Pristup za korisnike zasnovan je na organizacijskim potrebama. Pristup lokacijama u kojima postoji ograničenje kretanja je dozvoljen samo korisnicima s posebnim ovlastima.
Osjetljivi informacijski resursi moraju biti smješteni u posebno osiguranim dijelovima radne okoline. Izbor i osiguranje takvih prostora, smještaj opreme i radni uvjeti u takvim prostorima moraju uzeti u obzir sigurnosne rizike.

Pristup informacijskim resursima
Članak 17.

Pravo pristupa informacijama, informacijskim resursima i procesima informacijskog sustava, uključujući i Internet, može biti dodijeljeno samo temeljem dozvole nadležnog voditelja. Svakom korisniku informacijskog sustava mora biti dodijeljeno jedinstveno korisničko ime, a svako korisničko ime mora imati i svoju lozinku. Korisnik je obavezan čuvati svoju lozinku i ne odavati je drugim osobama.

Zaštitne kopije podataka („back-up“)
Članak 18.

Potrebno je redovito izrađivati zaštitne kopije produkcijskih podataka. Odgovornost i upute za izradu zaštitnih kopija mogu biti specificirani posebnim procedurama.

Potrebno je bilježiti evidenciju o postupku redovite izrade zaštitnih kopija. Zaštitne kopije moraju biti spremljene na primjeren način, u dovoljnom broju kopija, a prema potrebi i izvan glavne lokacije Društva. Potrebno je povremeno uvježbavati postupak povratka podataka sa zaštitnih kopija.

Sigurnost osobnih računala
Članak 19.

Obrada, pohrana i korištenje podataka na osobnim računalima moraju biti provedeni tako da se spriječe sigurnosni rizici. Zaštita resursa na osobnim računalima određena je razinom osjetljivosti resursa i njihovim značajem za Društvo.

Nije dozvoljena instalacija bilo kakvih programskih paketa ili sklopovskih uređaja na osobnim računalima bez suglasnosti voditelja IT odjela.

Korisnici osobnih računala moraju slijediti sve upute za zaštitu od računalnih virusa ili drugih destruktivnih programa. U slučaju pojave računalnog virusa ili drugih destruktivnih programa, korisnici moraju odmah obavijestiti nadležnu osobu.

Zaštita od virusa
Članak 20.

Potrebno je definirati i provesti mjere zaštite od virusa i drugih destruktivnih programa na svim osobnim računalima, mrežnim serverima, mail serverima i serverima koji omogućuju pristup Internetu. Mjere zaštite od virusa podrazumijevaju i korištenje primjerenog programa za zaštitu od virusa. Korisnici moraju biti upoznati s procedurom zaštite od virusa.
Potrebno je provjeravati svaku datoteku na elektroničkom mediju poznatog ili nepoznatog porijekla, a posebno one datoteke koje pristignu putem mreže.

Programi koji služe za zaštitu od virusa moraju biti redovito ažurirani i nadograđivani.

Korisnici ne smiju imati mogućnost isključivanja ili onemogućavanja programa za zaštitu od virusa.

V. PRISTUP I KORIŠTENJE RAČUNALNIM SUSTAVIMA
Članak 21.

Ovaj Pravilnik daje upute o načinu korištenja računalnog sustava i drugih informatičkih resursa društva. Cilj ovog Pravilnika je osigurati djelotvorno, efikasno, etično i zakonski primjereno korištenje resursa informacijskog sustava od strane svih zaposlenika i/ili vanjskih partnera društva koji koriste resurse informacijskog sustava društva (u daljnjem tekstu: Korisnik/Korisnici).

Računalni sustav i drugi informatički resursi uključuju sva računala, servere ili mrežne uređaje koji su instalirani unutar računalne infrastrukture Društva ili kojima se može pristupiti putem računalne infrastrukture Društva.

Korištenje informatičkih resursa podrazumijeva upotrebu i obradu podataka ili programa koji se nalaze na tako definiranim resursima te upotrebu podataka ili programa koji se nalaze na magnetnim trakama, disketama, CD-ROM ili drugim medijima za pohranu podataka za koje skrbi ovlaštena osoba.

Članak 22.

Korisniku se mogu dodijeliti ovlasti za pristup informacijskom sustavu s ciljem obavljanja redovite radne aktivnosti iz djelokruga poslovnog procesa u kojem sudjeluje Korisnik.
Za određivanje nivoa prava pristupa informacijskom sustavu je nadležan neposredno nadređeni voditelj Zaposlenika, a sama dodjela prava se vrši od zaposlenika IT odjela ili druge ovlaštene osobe.

Ovlasti za pristup resursima mogu biti korištene samo za namjenu za koju su i dodijeljene.

Članak 23.

Svi informatički resursi koji se koriste u poslovnom procesu, uključujući računalne programe i odgovarajuće podatke, smatraju se vlasništvom/imovinom Društva.

Osobe nadležne za provedbu mjera sigurnosti informacijskog sustava ili druge osobe koje ovlasti Uprava društva mogu pristupiti i pročitati materijale koje Korisnici kreiraju, pohranjuju, šalju ili primaju računalima društva, internetom ili bilo kojom drugom računalnom mrežom, sve sukladno postupku iz čl 47. ovog Pravilnika.

Korisnici prihvaćaju mogućnost da Društvo provede nadzor nad korištenjem informatičkih resursa. Takav nadzor može biti automatski ili posredstvom ovlaštene osobe.

Članak 24.

Korisnik ne smije otkriti drugim osobama načine pristupa na sustav. Prethodna odredba se naročito odnosi na podatke o pristupu na VPN ulaze društva ili druge oblike udaljenog pristupa.

Članak 25.

Korisnici ne smiju neovlašteno kopirati službeni software na kojemu je zaštićeno pravo korištenja, osim pod uvjetima koji su dozvoljeni zakonskim odredbama ili eksplicitnom dozvolom od strane proizvođača.

Članak 26.

Korisnici ne smiju raditi kopije konfiguracijskih i sistemskih datoteka. Korisnici ne smiju neovlašteno pristupati sistemskim i konfiguracijskim datotekama, niti smiju takve datoteke koristiti za namjenu koja je različita od osnovne namjene.
Konfiguracijske i sistemske datoteke mogu se dati na uvid drugim osobama samo uz ovlaštenje voditelja IT odjela (ili osobe koju on ovlasti) ili Uprave društva.

Članak 27.

Korisnici ne smiju instalirati nikakav programski paket, interni sklopovski uređaj ili periferni sklopovski uređaj na osobna računala društva bez suglasnosti voditelja IT odjela ili druge ovlaštene osobe.
Prijenosna računala mogu biti spojena na mrežu Društva samo prema tehničkim zahtjevima propisanim od IT odjela ili druge ovlaštene osobe.
Korisnici ne smiju kopirati s vanjskih računala, instalirati ili izvoditi programe koji imaju za cilj otkrivati sigurnosne slabosti na sustavu (na primjer programi za dekodiranje lozinki) osim u slučajevima planirane sustavne kontrole prometa i sadržaja u lokalnoj mreži u svrhu optimizacije sustava i poslovnih procesa.

Članak 28.

U trenutku kada Korisnik privremeno napušta radno mjesto treba završiti rad u svim aktivnim programima.
Ako se koristi "screen saver" program s ugrađenom zaštitom pomoću lozinki onda se kod kraćih izlazaka ne mora postupati prema odredbi iz prethodnog stavka.

Korisnik mora izvijestiti nadležne osobe o svakom primijećenom nedostatku u sustavu računalne sigurnosti, te o svakoj zloupotrebi i kršenju sigurnosne politike informacijskog sustava.
Nadležne osobe su neposredni voditelj ili IT odjel. Nadležne osobe se izvješćuju putem elektronske pošte ili drugim pisanim putem.

Članak 29.

Korisnik je obvezan:
- pri pristupu računalnim sustavima Društva koristiti samo korisničke identifikacije (USERID) koje mu je dodijelilo Društvo,
- isključiti se s računalnih sustava Društva odmah nakon završetka rada,
- držati u tajnosti lozinku, pristupne kodove (PIN) i dr. koji su dodijeljeni njegovoj korisničkoj identifikaciji,
- pridržavati se naputaka (pismenih ili usmenih) Društva koji se odnose na njegov pristup računalnim sustavima Društva,

- u slučaju saznanja o bilo kakvim incidentima glede sigurnosti, o nedostacima ili sumnjivim aktivnostima na računalnim sustavima Društva, odmah obavijestiti Društvo i u potpunosti surađivati s Društvom kako bi se neželjene posljedice što prije uklonile.

Članak 30.

Korisniku se zabranjuje:
- dopustiti drugima pristup računalnim sustavima Društva uporabom svoje korisničke identifikacije,
- namjerno pristupati informacijama, podacima ili računalnim sustavima, osim onima za koje ga je Društvo ovlastilo,
- namjerno širiti viruse, elektronička lančana pisma i druge zlonamjerne računalne kodove na računalne sustave Društva,
- instalirati software, osim onoga koji je potreban za izvršenje poslova koje je Društvo ugovorilo.

VI. KORIŠTENJE INTERNETA I ELEKTRONSKE POŠTE

Članak 31.

Internet se smatra značajnim poslovnim resursom, a elektronička pošta i značajnom komponentom informacijskog sustava Društva. Zaposlenici Društva se potiču na korištenje i unaprjeđenje mogućnosti primjene Interneta.
Internet se može koristiti prije svega za poslovnu namjenu.

Cilj ovog Pravilnika je osigurati djelotvorno, efikasno, etično i zakonski primjereno korištenje elektroničke pošte i Interneta.

Članak 32.

Društvo nije odgovorno za materijal koji Zaposlenici pregledavaju ili spuštaju s Interneta. Zaposlenici preuzimaju rizik za sve eventualne posljedice do kojih bi moglo doći uslijed pristupa i prijema neprikladnog ili uvredljivog sadržaja.

Članak 33.

Zaposlenici smiju pristupati Internetu isključivo preko računalne mreže Društva i putem odgovarajuće infrastrukture vatrozidne zaštite.
Direktan pristup Internetu (nekontroliran pristup) strogo se zabranjuje.

Članak 34.

E-poštom nije dozvoljeno slati materijal koji ima lažljiv, uznemiravajući, neugodan, seksualno eksplicitan, nepristojan, ili zakonski nedozvoljen sadržaj.

Materijal opisan u prvom stavku nije dozvoljeno preuzimati ili spuštati s Internet poslužitelja.

Članak 35.

Društvo može koristiti specijalizirane programe koji imaju svrhu identifikacije i blokiranje pristupa svim Internet serverima sa sadržajima koji nisu primjereni poslovnim procesima Društva.

U slučaju da se Zaposlenik ipak slučajno poveže na servere s neprimjerenim sadržajem, dužan je trenutno prekinuti takvu vezu.

Članak 36.

Nije dozvoljeno koristiti Internet kroz aktivnosti koje uzrokuju neprimjereno zauzeće računalnih resursa na štetu drugih zaposlenika.

Takva aktivnost uključuje, između ostalog, slanje masovnih ili lančanih e-mail poruka, sudjelovanje u chat grupama ili kreiranje značajnog prometa na bilo koji drugi način.

Članak 37.

Zaposlenici preuzimaju odgovornost za sve posljedice koje bi mogle proizaći uslijed nepridržavanja zakona o intelektualnom vlasništvu i drugih pravnih pravila vezano za software, datoteke, grafiku, dokumente ili druge oblike intelektualnog vlasništva.

Članak 38.

Zaposlenici su dužni pridržavati se svih procedura zaštite od virusa kod prijema datoteka putem Interneta, a naročito kod prijema e-mail poruka s privitkom.

Nije dozvoljeno izvoditi programe primljene u privitku e-mail poruka.

Ako se putem Interneta prihvati datoteka s programskim kodom namijenjenim za upotrebu u poslovnim procesima Društva, onda se takva datoteka smije instalirati i izvoditi tek nakon provedenog postupka prihvaćanja i odobravanja (testiranja) programskih proizvoda.

Članak 39.

Zaposlenik ne smije slati ne zahtjevane e-mail poruke osobama s kojima prethodno nije uspostavljen poslovni odnos, osim u slučaju pismenog odobrenja odgovorne osobe.

Članak 40.

Zaposlenik ne smije u e-mail poruci mijenjati sadržaj polja koje označava porijeklo poruke (polje “From”/”Od”). Nije dozvoljena komunikacija u kojoj je pošiljatelj anoniman ili koristi pseudonim. Zaposlenik se mora ispravno identificirati u svakom obliku elektronske komunikacije.

Članak 41.

Poruke koje zaposlenici stavljaju na mailing liste ili „news grupe“ moraju uključivati i izjavu da ta poruke ne izražava i službeni stav Društva.

Članak 42.

Društvo zadržava pravo, ali ne i dužnost (u slučajevima predviđenim ovim Pravilnikom i drugim aktima Društva) nadzora korištenja svakog aspekta informacijskog sustava Društva, uključujući, između ostalog, nadzor nad Internet adresama koje zaposlenici posjećuju, nadzor nad komunikacijom sa „chat“ i „news grupama“, pregled materijala koji se spušta s Interneta, te pregled e-mail poruka koje se primaju ili šalju Internetom, sve u skladu s postupkom iz čl. 47 ovog Pravilnika.

Politika „čistog stola i čistog ekrana“
Članak 43.

Politika čistog stola i čistog ekrana uzima u obzir klasifikaciju informacija, zakonske zahtjeve i ugovorene obveze, te odgovarajuće aspekte rizika i kulture unutar Društva. Zaposlenici se trebaju pridržavati slijedećeg:
a) informacije koje su osjetljive ili kritične za poslovanje npr. papiri ili mediji za elektroničku pohranu informacija, trebaju biti zaključani (idealno u sigurnom kabinetu ili drugom obliku sigurnog namještaja) na izdvojenom mjestu kada nisu potrebni, a posebno kada u uredu nema nikoga,
b) kada su bez nadzora, računala i terminali trebaju biti u statusu «log-off» ili zaštićena s mehanizmima zaključavanja tipkovnice i ekrana koji imaju lozinku, token ili drugi način autentifikacije,
c) kada se ne koriste, računala trebaju biti zaštićena ključem, lozinkom ili na drugi način od neovlaštenog pristupa,
d) kod kopiranja, skeniranja i fotografiranja dokumenata koji su klasificirani kao povjerljivi, treba voditi posebnu pažnju da takvi dokumenti ili njihove elektroničke kopije ne postanu dostupni neovlaštenim osobama,
e) dokumenti koji sadrže osjetljive ili klasificirane informacije trebaju odmah biti sklonjeni s printera,
f) u tijeku radnog vremena dokumenti označeni kao poslovna tajna i drugi izvori podataka kao i sredstva automatske obrade dokumenata ne smiju se ostavljati bez nadzora,
g) nakon završetka radnog vremena svi zaposlenici obvezni su dokumente označene kao poslovna tajna i druge izvore podataka, pečate, žigove i štambilje, prijenosne informatičke medije (DVD, USB memorije, diskovi i slično) držati zaključane u ladicama ili ormarima u radnim prostorima Društva.

VII. UPRAVLJANJE SIGURNOSNIM INCIDENTIMA

Članak 44.

Svrha procedure je osiguravanje brzog obavještavanja osoba odgovornih za informacijsku sigurnost o mogućim ili trenutnim sigurnosnim događajima i incidentima te definiranje aktivnosti za upravljanje sigurnosnim incidentima.

Procedura se primjenjuje na sve sustave i/ili poslovne procese društva.

Incidenti informacijske sigurnosti uključuju ali nisu ograničeni na: gubitak servisa (npr. struja, voda, Internet), opreme ili resursa greške u radu sustava i preopterećenje, ljudske greške, nepoštivanje politika, procedura, naputaka i ostale važeće dokumentacije povreda fizičke sigurnosti nekontrolirane promjene na sustavu greška u radu hardvera ili software-a povreda pravila pristupa.

Članak 45.

a) Klasifikacija incidenata prema prioritetu:

S1 - Vrlo visok prioritet podrazumijeva trenutan i kontinuirani napor dok se ne otkloni uzrok incidenta. Koriste se svi raspoloživi oblici komuniciranja kao i usluge vanjskih partnera.

S2 - Visok prioritet podrazumijeva trenutan odgovor tehničke podrške, procjena situacije i ukoliko je potrebno angažiranje drugih članova tima koji rade na incidentima umjerenog i niskog prioriteta.

S3 - Umjeren prioritet podrazumijeva odgovor korištenjem standardnih procedura uz nadzor i upravljanje putem standardnih upravljačkih struktura.

S4 - Nizak prioritet podrazumijeva odgovor korištenjem standardnih procedura.

b) Klasifikacija incidenata prema utjecaju na poslovanje:

Veliki utjecaj - incidenti koji imaju trenutni utjecaj na poslovanje Društva ili na pružanje usluga korisnicima.
Srednji utjecaj - incidenti koji imaju značajan utjecaj na poslovanje Društva. Ukoliko se pravovremeno ne pristupi njihovom rješavanju mogu imati veliki utjecaj na poslovanje društva ili na pružanje usluga korisnicima.
Mali utjecaj - incidenti koji po svom obimu ne pokazuju mogućnost širenja ili značajnijeg utjecaja na poslovanje društva ili na pružanje usluga Korisnicima.

VII.I. Procedura za prijavu incidenta
Članak 46.

Incident može biti prijavljen putem:
- pisanim zahtjevom,
- e-mailom,
- telefonom,
- mobilnim telefonom.

Prijava incidenata vrši se prema vrsti incidenta kojoj pripada.
Kada bilo koji zaposlenik primijeti sigurnosni problem ili posumnja da je sigurnost informacijskog sustava upitna, mora hitno obavijestiti voditelja IT odjela ili neposredno nadređenu osobu.
Zaposlenik mora zabilježiti sve informacije koje bi mogle biti od koristi prilikom rješavanja problema i daljnjih akcija (poruke na zaslonima, okolnosti oko događaja...)
Zaposlenik koji primijeti sigurnosni propust ili nedostatak ne smije nikad samostalno probati dokazati postojanje istog, osim u slučajevima kada ima službeno odobrenje.

Detalji koji se bilježe su:
- osoba koja je prijavila incident, datum i vrijeme prijave incidenta
- tip incidenta i utjecaj incidenta (veliki, srednji, mali),
- sustav na kojem je nastao incident,
- kratak opis incidenta,
- poduzete radnje,
- osoba koja rješava incident,
- datum i vrijeme rješavanja
- komentar ili opaska.

Nakon što nadležna osoba zaprimi informaciju o sigurnosnom incidentu, mora čim prije započeti sa rješavanjem incidenta.
Svi dokazi o incidentu, bilo u papirnatom ili elektronskom obliku, moraju biti adekvatno prikupljeni i zaštićeni od namjerne ili nenamjerne promjene.

Nakon poduzimanja određenih aktivnosti s ciljem rješavanja incidenta, mora se obavezno provjeriti funkcionalnost sistema.

Voditelj IT odjela ili druga nadležna osoba će o svim većim incidentima obavijestiti Upravu.

Ukoliko je potrebno, Uprava će obavijestiti nadležna državna tijela i/ili eventualno oštećene osobe.

Bez prethodne dozvole Uprave Društva, Zaposlenici Društva ne smiju javno objavljivati podatke o pojavi sigurnosnih incidenata, problema ili ranjivosti sustava i računalne mreže Društva. Izuzetak predstavljaju slučajevi u kojima je Društvo zakonom obavezno objaviti ove podatke.

Provjera rada sustava
Članak 47.

Društvo zadržava pravo nadzora i bilježenja svih aktivnosti na računalnim resursima, te provođenja redovitih provjera pridržavanja sigurnosne politike.

Voditelj sigurnosti informacijskog sustava ili druga ovlaštena osoba trebala bi periodički provjeravati stanje sigurnosti pojedinih komponenti informacijskog sustava, sistemske zapise o radu informacijskog sustava, radu korisnika i druge sistemske podatke u cilju otkrivanja nepridržavanja Pravilnika, upravljanja rizicima i otkrivanja različitih odstupanja koja bi mogla uzrokovati sigurnosne incidente.

Bilježenje aktivnosti na računalnim resursima može obuhvatiti i bilježenje osobnih podataka korisnika koje korisnici kreiraju, spremaju, šalju ili primaju putem računala tvrtke, a koji nisu vezani za poslovne procese Društva.

Društvo zadržava pravo provjere svake datoteke ili poruke elektroničke pošte koja je kreirana, spremljena ili proslijeđena računalnim resursima Društva, što uključuje i pravo provjere datoteka ili poruka s privatnim sadržajem koje se nalaze u osobnim mapama ili direktorijima korisnika.

Ovo pravo se može koristiti samo u slučajevima kada postoji jasna indicija o nepridržavanju odredbi ovog Pravilnika ili drugih općih akata Društva, zakonskih odredbi i u slučaju legitimnog interesa Društva (npr. sigurnosne ugroze sustava i sl.).
Provjera se može obaviti samo uz suglasnost neposrednog rukovoditelja, a na zahtjev voditelja sigurnosti informacijskog sustava ili voditelja IT odjela ili druge ovlaštene osobe Društva.

VIII. OBVEZA POVRATA INFORMACIJA
Članak 48.

Sva materijalna imovina koja sadrži informacije u svezi s ugovorom o radu i radnim odnosom, vlasništvo je Društva, pa je zaposlenik obvezan:
Po prestanku radnog odnosa, ali i prije toga na zahtjev Društva, vratiti Društvu svu imovinu koja sadrži bilo koju vlasničku ili poslovnu tajnu Društva, uključujući i sve kopije, izvatke i sažetke, bez zadržavanja bilo kakvih kopija za sebe,

- Po prestanku radnog odnosa, ali i prije toga na zahtjev Društva, izbrisati sve digitalne kopije vlasničkih i poslovnih tajni Društva sa svojeg diska, te sa svih drugih svojih medija ili medija Društva,
- Po prestanku radnog odnosa, ali i prije toga na zahtjev Društva, vratiti Društvu svu materijalnu imovinu koju je dobio na korištenje s osnova radnog odnosa u Društvu.

IX. ZAKLJUČNE ODREDBE
Članak 49.

Povreda dužnosti čuvanja poslovne tajne smatra se teškom povredom obveze iz radnog odnosa radi koje Društvo može počinitelju izvanredno otkazati ugovor o radu.

Ukoliko je zbog neovlaštenog priopćavanja podataka koji se smatraju tajnom za Društvo nastala šteta, protiv osobe koja je povrijedila dužnost čuvanja tajne može se pokrenuti postupak za naknadu štete pred nadležnim sudom.

Prilikom sklapanja ugovora o radu može se ugovoriti ugovorna kazna za slučaj povrede čuvanja poslovne tajne. U slučaju da zaposlenik povrijedi dužnost čuvanja tajne Društvo ima pravo zahtijevati cijeli iznos ugovorne kazne i u slučaju kad njezin iznos premašuje štetu koju je pretrpio kao i kad nije pretrpio nikakvu štetu.

Povreda dužnosti čuvanja poslovne tajne može za počinitelja rezultirati i kaznenom odgovornošću.

Osim već ranije u ovom članku navedenih povreda, nepridržavanje bilo koje od odredbi ovog Pravilnika smatra se povredom radne obaveze za koju se može dati izvanredan otkaz ili otkaz uvjetovan skrivljenim ponašanjem zaposlenika, te će se provesti utvrđivanje odgovornosti zaposlenika za svaki pojedinačni slučaj nepridržavanja bilo koje od uputa ili odredbe ovog Pravilnika.

Nepridržavanje odredbi ovog Pravilnika od strane vanjskih korisnika i partnera može se smatrati povredom ugovornih obaveza koja je razlog za raskid ugovora.

Članak 50.

Za pitanja koja nisu regulirana ovim pravilnikom primjenjuju se odluke Uprave Društva.
Ovaj se Pravilnik mijenja i dopunjuje na način propisan za njegovo donošenje.

Članak 51.

Ovaj Pravilnik stupa na snagu osmoga dana od dana njegove objave na oglasnoj ploči Društva.

Ovaj Pravilnik dostupan je svim zaposlenicima Društva i drugim ovlaštenim osobama na koje se primjenjuje.

Samobor, 01. siječnja 2020.

_____