Pravilnik o prihvatljivom korištenju informacijskog sustava i određivanju nadležnosti i odgovornosti u informacijskom sustavu

Zagreb, 31.03.2023.

SADRŽAJ

1. UVOD I OPSEG PRIMJENE

Pravilnik o prihvatljivom korištenju informacijskog sustava Društva (dalje u tekstu: Pravilnik) pobliže određuje i regulira način korištenja informacijskog sustava Društva, a u svrhu zaštite zaposlenika, putnika i poslovnih partnera od namjernih ili nenamjernih štetnih ili nezakonitih aktivnosti.

S obzirom da rizici u radu i korištenju informacijskog sustava neposredno ovise o i postupanju korisnika informacijskog sustava, cilj ovog Pravilnika je propisati mjere za sigurno, djelotvorno, etično i zakonski primjereno korištenje informacijskog sustava Društva koje korisnici moraju provoditi u radu s resursima informacijskog sustava Društva.

Odredbe ovog Pravilnika se primjenjuju kod pristupa i korištenja svih resursa informacijskog sustava Društva te servisa dostupnih resursima informacijskog sustava Društva putem Interneta.

Odredbe ovog Pravilnika se odnose na sve zaposlenike Društva, vanjske suradnike, volontere, zaposlenik drugog poslovnog subjekta s kojim Društvo surađuje temeljem ugovora o poslovnoj suradnji ili druge osobe kojima je odobren pristup resursima informacijskog sustava Društva (dalje u tekstu: Korisnici).

2. PRISTUP INTERNETU

2.1 Informacijski sustav Društva

Informacijski sustav Društva uključuje svaki hardverski ili programski resurs – poslužitelje, mrežne uređaje, aplikacije, informacijske servise, podatke i slično, koji su u vlasništvu Društava ili ih Društvo koristi.

Korištenje informacijskog sustava podrazumijeva upotrebu podataka ili aplikacija koja se nalaze na računalnim resursima Društva, na prijenosnim medijima za pohranu podataka u vlasništvu Društva ili koje Društvo koristi, na vanjskim mrežnim resursima dostupnim i odobrenim za korištenje u poslovnim procesima Društva.

2.2 Internet i servisi dostupni putem Interneta

Internet kao javno dostupna globalna mreža predstavlja značajan, a za neke poslovne procese i neophodan, resurs u radu informacijskog sustava Društva.

Odredbe ovog pravilnika se primjenjuju na sve aspekte pristupa i korištenja Interneta te servisa dostupnih putem Interneta, kako putem resursa informacijskog sustava Društva, tako i izvan ovih resursa u slučajevima kad neka osoba nastupa kao zaposlenik Društva.

2.3 Odgovornost korisnika

Korisnici informacijskog sustava su odgovorni za profesionalnu, etičku i zakonitu upotrebu resursa informacijskog sustava.

Informacijski sustav Društva smije se koristiti isključivo za svrhu provedbe poslovnih procesa Društva.

Izuzetno, dozvoljava se upotreba resursa informacijskog sustava Društva i u privatne svrhe, ali u ograničenom trajanju i razumnom opsegu.

Korisnici ne smiju kreirati ili pohranjivati materijale čiji je sadržaj uznemiravajući, neugodan, opscen, seksualno eksplicitan, pornografski, nepristojan, klevetnički ili na bilo kakav način neprihvatljiv ili zakonski nedozvoljen.

Korisnici ne smiju sudjelovati u aktivnostima čija je namjera uznemiravati ili vrijeđati druge osobe, niti je dozvoljeno na bilo koji drugi način širiti materijale uvredljivog sadržaja.

Korisnik je dužan koristiti resurse informacijskog sustava Društva na način koji će spriječiti ugrožavanje dostupnosti, povjerljivosti i cjelovitosti ovih resursa, provodeći propisane mjere zaštite te temeljem drugih saznanja o mjerama zaštite računalnih resursa.

Korisnici preuzimaju odgovornost za sve posljedice koje bi mogle proizaći uslijed nepridržavanja zakona kojima se uređuje pravo korištenja za softver, datoteke, grafiku, dokumente ili druge oblike intelektualnog vlasništva.

Korisnici su dužni provoditi mjere zaštite osobnih podataka sukladno odredbama Politike zaštite osobnih podataka Društva.

3. PRISTUP KORISNIKA INFORMACIJSKOM SUSTAVU

3.1 Korisnički računi za pristup informacijskom sustavu

Korisnici moraju pristupati informacijskom sustavu isključivo upotrebom vlastitih službeno odobrenih korisničkih računa.

Korisnici mora svoje ovlasti za pristup informacijskom sustavu koristiti isključivo kroz vlastiti rad i ne smiju nikome drugome omogućiti njihovo korištenje.

Svaki je Korisnik odgovoran za sve transakcije i druge aktivnosti nad resursima informacijskog sustava koje su provedene korištenjem njegovog korisničkog računa.

Mogućnost pristupa Korisnika sadržaju koji nije predviđen ulogom Korisnika u poslovnom procesu ili za koju nema odobrenje pristupa, ne podrazumijeva i dozvolu za takvu akciju, te je Korisnik dužan suzdržati se od pristupa takvim podacima.

Korisnici se smiju povezati na računalnu mrežu Društva isključivo resursima Društva koji su odobreni za korištenje u navedenu svrhu.

3.2 Zaštita podataka o korisničkoj autentikaciji

U slučaju kada je korisničkom računu pridijeljena odgovarajuća lozinka ili drugi autentikacijski podaci, Korisnik je odgovoran za izbor i čuvanje lozinki za pristup informacijskom sustavu.

Korisnik ne smije lozinke ili druge autentikacijske podatke otkriti drugim osobama.

Korisnici ne smiju držati lozinke u pisanom obliku niti ih smiju pohraniti na računalu ili slati elektroničkom poštom. Izuzetno, lozinke se smiju pohraniti i na računalu ali isključivo uz korištenje prikladnih i prethodno odobrenih programa za čuvanje i zaštitu lozinki.

Korisnik je dužan redovito mijenjati lozinke.

Korisnik mora poštovati slijedeće smjernice kod izbora i primjene lozinki za zaštitu vlastitih korisničkih ovlasti i zaštitu dijelova informacijskog sustava Društva:

- Lozinke ne mogu sadržavati korisničko ime ili puno ime
- Maksimalna starost lozinke je 90 dana
- Minimalna duljina lozinke je 8 znakova
- Sustav pamti zadnjih 12 lozinki (identičnu lozinku nije moguće ponavljati)
- Minimalna starost lozinke je 0 dana
- Maksimalna starost lozinke je 90 dana
- Nakon 6 neispravnih unosa lozinke korisnički račun se zaključava na 30 minuta (nakon 30 minuta automatski se otključava)
- Definirana je i kompleksnost lozinke, lozinka mora sadržavati 3 od 4 uvjeta: Veliko slovo (A do Z), Malo slovo (a do z), Broj (0 do 9), specijalni karakter (npr. !, $, #, %)

Lozinka koja dolazi kod početne instalacije programskih paketa ili uređaja obavezno mora biti zamijenjena.

4. OBAVEZA ZAŠTITE RAČUNALNIH RESURSA

4.1 Zaštita osobnih računala

Prijenosna računala, mobilni uređaji, periferni uređaji i slična sklopovska oprema smiju se povezati na mrežu Društva isključivo uz odobrenje Sektora upravljanja informacijskim tehnologijama.

Korisnici ne smiju instalirati nikakav programski paket, interni ili periferni sklopovski uređaj na osobno računalu koji koriste. Izuzetno, instalacija ovih resursa moguća je isključivo s odobrenjem Sektora upravljanja informacijskim tehnologijama.

Korisnici ne smiju neovlašteno pristupati sistemskim datotekama i konfiguracijskim postavkama, ne smiju ih mijenjati, kopirati, otkrivati njihov sadržaj drugim osobama niti koristiti za namjenu koja je različita od osnovne namjene.

Korisnici ne smiju svjesno provoditi akcije koje nepotrebno zauzimaju resurse sustava ili slabe performanse rada sustava, niti smiju sudjelovati u akcijama koje drugim Korisnicima sprječavaju pristup informacijskom sustavu.

Korisnici ne smiju provoditi akcije kojima je cilj pronalaženje nedostataka ili izbjegavanje standardnih mjera sigurnosti osobnog računala te informacijskog sustava Društva u cjelini.

Korisnici se moraju pridržavati uputa Sektora za upravljanje informacijskim tehnologije o zaštiti od računalnih virusa i drugih malicioznih programa, te spriječiti bilo kakvu aktivnost koja uvećava rizike unošenja računalnih virusa i malicioznih programa.

Korisnici smiju kriptirati podatke koje pohranjuju na osobnim računalima ili na podatkovnim poslužiteljima isključivo uz suglasnost Sektora upravljanja informacijskim tehnologijama, upotrebom isključivo odobrenog softvera za te sukladno uputama o kriptiranju podataka.

4.2 Fizička zaštita resursa informatičkog sustava

U trenutku kada Korisnik privremeno napušta radno mjesto, dužan je pokrenuti program koji sprječava pristup osobnom računalu tehnikom zaključavanjem ekrana ili odjaviti rad na računalu.

Prijenosni podatkovni mediji (USB, prijenosi diskovi, DVD, CD ili slični resursi) te papirni dokumenti s osjetljivim podacima moraju izvan upotrebe biti pohranjeni na lokaciji na kojoj neće biti fizički dostupni neovlaštenim osobama.

Korisnici kojima su dodijeljena prijenosna računala i/ili mobilni uređaju odgovorni su za zaštitu i sigurnu upotrebu ovih uređaja, osobito na lokacijama izvan poslovnih prostora Društva.

Pri korištenju prijenosnih računala i/ili mobilnih uređaja izvan radnog mjesta a naročito u javnim prostorima, Korisnik mora spriječiti neovlašteni uvid drugih osoba u sadržaj prikazan na ekranima uređaja.

5. ZAŠTITA PODATAKA, ZAŠTITA INTELEKTUALNOG VLASNIŠTVA I SOFTVERA

5.1 Povjerljive poslovne informacije

U informacijskom sustavu Društva provodi se klasifikacija podataka i definira način označavanja i rukovanja klasificiranim podacima na sljedeći način:

Naziv razine	Karakteristika	Mjere zaštite	Primjer
Tajno	Samo za grupu imenovanih osoba, iznimno velika financijska šteta i/ili gubitak ugleda	Kontrola pristupa uz pouzdanu autentikaciju i bilježenje svih aktivnosti. Enkripcija podataka u pohrani je obavezna u spremanju podataka na prijenosna računala i u prijenosu podataka. Prema potrebi pristup omogućen isključivo uz prisutnost dvije osobe. Dokumentacija u papiru se pohranjuje u zaključane vatrootporne ormare.	-preliminarna bilanca -kvartalne i godišnje brojke prije objavljivanja -zapisnik sa sastanka Uprave Društva -detaljni izvještaji o informacijskoj sigurnosti
Povjerljivo	Samo za ograničenu grupu ljudi, kršenje ugovora i/ili zakona nosi visoku vjerojatnost značajnih gubitaka (kazne, pravne radnje), ostvarivanje prednosti za konkurente, vjerojatni gubitak reputacije	Kontrola pristupa uz bilježenje svih aktivnosti. Preporučena je enkripcija podataka u pohrani, a obavezna u prijenosu podataka. Dokumentacija u papiru se pohranjuje u zaključane ormare ili ladice.	-informacije o klijentima -svi osobni podaci klijenata ili drugih ispitanika -pojedinosti o novim proizvodima prije objavljivanja -kartični podaci
Interno	**Osnovna razina** Dijeljenje između zaposlenika Društva, izravni financijski gubici su vrlo malo vjerojatni, reputacijski utjecaj	Kontrola pristupa. Preporučena enkripcija u slučaju slanja izvan Društva.	-interna poslovna komunikacija -bilješke -zapisnici sa sastanka -interni dokumenti -specifikacije
Javno	Mogu biti javno objavljene		-sadržaj javnih web-stranica -priopćenja za javnost -opisi proizvoda i brošure

Svi podaci smješteni unutar resursa informacijskog sustava smatraju se povjerljivim.

Ispis, objava, distribucija ili obrada povjerljivih poslovnih podataka je dozvoljena isključivo unutar poslovnog procesa u kojem su definirane takve aktivnosti ili uz suglasnost osobe odgovorne za ove podatke, kao i uz poslove definirane sistematizacijom radnih mjesta.

5.2 Kartični podaci

Nije dozvoljeno slanje brojeva kreditnih i debitnih kartica elektroničkom poštom Društva ili drugim komunikacijskim kanalima. Izuzetno, takve je podatke moguće slati isključivo ako su prije prijenosa kriptirani, sukladno uputama o kriptiranju podataka.

5.3 Sadržaj zaštićen autorskim pravima

Korisnici ne smiju neovlašteno kopirati sadržaj koji je označen kao intelektualno vlasništvo, ne smiju sudjelovati u aktivnostima neovlaštenog kopiranja i distribucije takvog sadržaja, niti smiju

takav sadržaj neovlašteno preuzimati sa Interneta ili ga na drugi način pohranjivati na informatičkim resursima Društva.

Izuzetno, Korisnici smiju kopirati ili pohranjivati sadržaje koji se smatraju intelektualnim vlasništvom samo na temelju odobrenja odgovornog rukovoditelja i to na temelju eksplicitne dozvole vlasnika sadržaja, na temelju ugovora s vlasnikom sadržaja ili na temelju nekog drugog akta koji podrazumijeva pristanak vlasnika sadržaja za takav postupak.

Odredbe iz ovog članka se osobito odnose na programske proizvode za koje Društvo ne posjeduje odgovarajuću licencu.

5.4 Zaštita intelektualnog vlasništva društva

Društvo je vlasnik autorskih prava na svim materijalima koje su radnici Društva, u okviru obavljanja svojih radnih zadataka dostavili putem Interneta ili Internet usluga.

Radnici moraju biti svjesni da su svi podaci koji su kreirani korištenjem informacijskih sustava tvrtke vlasništvo Društva i podliježu propisima koji reguliraju zaštitu intelektualnog vlasništva.

Društvo zadržava autorsko pravo i na materijalima koje su radnici Društva poslali i bilo kojim drugim elektroničkim putem.

6. KORIŠTENJE ELEKTRONIČKE POŠTE

6.1 Prihvatljivo korištenje elektroničke pošte

Korištenje servisa elektroničke pošte obuhvaća upotrebu elektroničke pošte za komunikaciju unutar Društva te za komunikaciju s vanjskim entitetima.

Korisnici su dužni servis elektroničke pošte koristiti uvažavajući odredbe o profesionalnoj, etičkoj i zakonitoj upotrebi resursa informacijskog sustava kako je definirana u članku 2.3 ovog Pravilnika.

Za slanje poruka elektroničke pošte s poslovnim sadržajem moraju se koristiti isključivo korisnički računi elektroničke pošte koji su otvoreni na poslužitelju Društva.

Korisnik ne smije u poruci elektroničke pošte mijenjati sadržaj polja koje označava porijeklo poruke. Nije dozvoljena komunikacija u kojoj je pošiljatelj anoniman ili koristi pseudonim. Korisnik se mora ispravno identificirati u svakom obliku elektronske komunikacije. Pod ispravnom identifikacijom podrazumijeva se i svaki grupni naziv ili adresa elektroničke pošte koja je u službenoj uporabi u Društvu.

Korisnik ne smije slati nezatražene poruke elektroničke pošte osobama koje nisu prethodno dale suglasnost za takvu aktivnost.

Nije dozvoljeno automatsko prosljeđivanje elektroničke pošte na bilo koju adresu elektroničke pošte koja ne pripada Društvu.

Nije dozvoljeno stvaranje ili posredovanje u slanju lančanih pisama, te piramidalnih shema bilo koje vrste.

6.2 Zaštita od socijalnog inženjeringa

Korisnici moraju s oprezom otvarati i čitati elektronički poštu koja dolazi s nepoznatih adresa ili ako dolazi s poznatih adresa ali u neuobičajenom kontekstu

Korisnici moraju obratiti pažnju i prema potrebi suzdržati se od daljnjih postupanja ako primljena električka pošta sadrži zahtjev za slanjem povjerljivih informacija kao što su korisnička imena,

lozinke, financijski podaci, ako poziva na bilo kakvu neuobičajenu aktivnost kao što su nalozi za plaćanje ili ako ima sličan neuobičajen sadržaj.

Korisnici moraju s osobitom pažnjom reagirati na elektroničku poštu koja sadrži poveznicu na Internet adresu te osobito ako poziva na otvaranje ove poveznice. U takvim se slučajevima Korisnici moraju suzdržati od otvaranja poveznice, osim u slučaju ako su nedvojbeno uvjereni da poruka elektroničke pošte dolazi od pouzdanog pošiljatelja.

Primitak poruka opisanih u prethodnim točkama ovog članka mora se prijaviti Sektoru upravljanja informacijskim tehnologijama.

7. PRISTUP INTERNETU I KORIŠTENJE INTERNET SERVISA

7.1 Korištenje Internet servisa

Korištenje Interneta i servisa dostupnih putem Interneta dozvoljeno je isključivo na način koji propisuje Sektor za upravljanje informacijskim tehnologijama te uvažavajući odredbe o profesionalnoj, etičkoj i zakonitoj upotrebi resursa informacijskog sustava kako je definirana u članku 2.3 ovog Pravilnika.

Korisnici ne smiju pristupati s mreže Društva Internet poslužiteljima na kojima je dostupan sadržaj koji je uznemiravajući, neugodan, seksualno eksplicitan, nepristojan, klevetnički ili bilo kakav način neprihvatljiv ili zakonski nedozvoljen, uključujući i slučajeve kada pristup takvim poslužiteljima s mreže Društva nije blokiran mjerama koje provodi Sektor za upravljanje informacijskim tehnologijama.

Korisnicima nije dozvoljeno prijavljivati na servise dostupne putem Interneta, koji omogućuju igre na sreću, kladionice i slično.

Korisnicima nije dozvoljeno prijavljivati na servise dostupne putem Interneta kao što su, među ostalim, mail, socijalne mreže, „cloud“ servisi i slično, a koji imaju osobnu namjenu, sa službenom adresom elektroničke pošte Korisnika.

U slučaju da Korisnik pristupa na javno dostupne Internet poslužitelje Društva s računala koji nisu u vlasništvu Društva onda Korisnik ne smije prihvatiti zahtjev za lokalnu pohranu korisničkog imena i zaporke ako bi takav zahtjev bio postavljen.

7.2 Korištenje socijalnih mreža

Korisnici se pozivaju na ograničeno, oprezno i promišljeno korištenje socijalnih mreža, pri čemu moraju objavljivati sadržaje isključivo u svoje osobno ime te izbjegavati rasprave o temama koje se odnose na Društvo. Korisnici se upozoravaju da sadržaj koji je objavljen na socijalnim mrežama ostaje dugotrajno dostupan.

Dozvolu za objavu sadržaja koji se odnosi na Društvo na socijalnim mrežama imaju isključivo djelatnici organizacijske jedinicu Društva nadležne za odnose s javnošću i/ili zastupanje društva na društvenim mrežama.

Prilikom objave sadržaja na socijalnim mrežama, uključujući i kada to rade u osobno ime, djelatnici Društva su obvezni su čuvati ugled i interese Društva. Nije dozvoljena objava podataka koji predstavljaju službenu tajnu Društva ili druge ograničeno dostupne informacije, kao i raspravljanje o temama koje se smatraju internim za Društvo.

Prilikom objave sadržaja na socijalnim mrežama, nije dozvoljeno navoditi i objavljivati podatke o putnicima, partnerima, dobavljačima i radnicima.

Sadržaj objavljen na socijalnim mrežama, diskusijskim grupama i forumima ne smije uključivati ni jedan podatak koji bi ukazivao na proizvođače, tipove ili modele komponenti informacijskog sustava Društva.

U slučaju da iz sadržaja na društvenoj mreži ili Internet forumima bude vidljivo da je osoba koja je objavila sadržaj zaposlenik Društva, onda objava mora obavezno uključivati izjavu da izraženo mišljenje ne predstavlja nužno i stav Društva. Od ove odredbe se izuzima sadržaj koji objavljuje organizacijska jedinica Društva nadležna za odnose s javnošću i/ili zastupanje društva na društvenim mrežama.

U slučaju da iz sadržaja na društvenoj mreži ili Internet forumima bude vidljivo da je osoba koja je objavila sadržaj zaposlenik Društva, onda objavljeni sadržaj ne smije biti uznemiravajući, neugodan, seksualno eksplicitan, nepristojan, klevetnički ili na bilo kakav način neprihvatljiv za druge osobe, odnosno zakonski nedozvoljen.

U slučaju da iz sadržaja na društvenoj mreži ili Internet forumima bude vidljivo da je osoba koja je objavila sadržaj zaposlenik Društva, Društvo može zahtijevati povlačenje i brisanje poruka koje nisu u skladu s poslovnim interesima ili poslovnom politikom Društva.

8. PRIJAVA INCIDENATA

Korisnici su dužni u najkraćem mogućem roku obavijestiti Voditelja sigurnosti IT sustava, Direktora upravljanja informacijskim tehnologijama ili druge ovlaštene osobe o svakom događaju koji upućuju na povredu sigurnosnih mjera propisanih ovim Pravilnikom te drugim internim aktima koji su funkciji zaštite informacijskog sustava.

Korisnici su dužni u najkraćem mogućem roku obavijestiti nadležnog rukovoditelja, Voditelja sigurnosti IT sustava ili Direktora upravljanja informacijskim tehnologijama o svim anomalijama u radu informacijskog sustava, a naročito o indikatorima nedozvoljenih aktivnostima na resursima informacijskog sustava.

Korisnik mora izvijestiti Voditelja sigurnosti IT sustava, Direktora upravljanja informacijskim tehnologijama ili druge ovlaštene osobe o svakom uočenom nedostatku u radu informacijskog sustava a naročito u mjerama sigurnosti informacijskog sustava.

9. SUGLASNOST O NADZORU

Društvo zadržava pravo nadzora korištenja svakog dijela informacijskog sustava, uključujući i nadzor nad poslužiteljima informacijskog sustava Društva, nadzor nad Internet adresama koje Korisnici posjećuju, nadzor nad servisima dostupnim putem Interneta ili društvenih mreža.

Nadzor informacijskog sustava uključuje i evidentiranje aktivnosti nad resursima informacijskog sustava te podatke o korisničkim računima koji su proveli ove aktivnosti.

Nadzor definiran prethodnim točkama primarno obuhvaća sistemske podatke o korištenju servisa ali nije isključena mogućnost uvida u sadržaj materijala koji se preuzima sa Interneta, te uvid u poruke koje se primaju ili šalju Internetom ili elektroničkom poštom. S obzirom da je nadzor informacijskog sustava je opravdan legitimnim interesom Društva, podrazumijeva se da Korisnici izražavaju privolu za eventualni uvid u osobne podatke u takvim slučajevima.

U slučaju analize sigurnosnih incidenata, postupak istrage može obuhvatiti i podatke pohranjene na osobnim, prijenosnim i mobilnim računalima Korisnika. U takvim slučajevima postupak istrage mora biti proveden na pravno valjan način.

Korisnici su dužni sudjelovati u postupku analize sigurnosnih incidenata ako je takva suradnja neophodna za ovaj postupak.

10. NADLEŽNOSTI I ODGOVORNOSTI U INFORMACIJSKOM SUSTAVU

10.1 Sudionici poslovnih procesa

Nadležnosti i odgovornosti pri korištenju informacijskog sustava Društva definiraju se za sljedeće sudionike poslovnih procesa:

- Uprava Društva
- Sektor upravljanja informacijskim tehnologijama
- Glavni korisnici
- Pružatelj informatičkih usluga
- Korisnici informatičkih usluga

10.1.1 Imovina informacijskog sustava Društva

Sastavni dijelovi informacijskog sustava Društva su imovina Društva.

Sastavni dijelovi informacijskog sustava mogu biti sva materijalna ili nematerijalna sredstva koja služe za prikupljanje, obradu, spremanje ili distribuciju informacija značajnih u poslovnim procesima (podaci, programski moduli, dokumentacija, ugovori, informatička oprema, dijelovi infrastrukture, pomoćne usluge i slično).

Društvo se prema komponentama informacijskog sustava koje su u vlasništvu drugih poslovnih subjekata, a koriste se u informacijskom sustavu Društva, odnosi kao prema imovini Društva.

10.1.2 Korištenje informacijskog sustava Društva

Korisnici informatičkih usluga su svi radnici Društva ili vanjski partneri Društva koji imaju pristup informacijskom sustavu Društva, sukladno svojim ulogama u poslovnim procesima Društva.

Svi Korisnici su dužni skrbiti se o sigurnosti informacijskog sustava Društva.

10.1.3 Načela za definiranje nadležnosti i odgovornosti

Nadležnosti i odgovornosti pri korištenju informacijskog sustava zasnovani su na sljedećim načelima:

1. Korisnik može imati pristup samo do podataka koji su nužni za obavljanje funkcija ovog korisnika iz redovitog poslovnog procesa
2. Ovlasti za korištenje informacijskog sustava moraju biti dodijeljene korisnicima prema načelu odvajanja radnih dužnosti

Načelo odvajanja radnih dužnosti podrazumijeva takvu dodjelu korisničkih prava iz kojih neće proizaći potpuna ovlast nad cjelokupnim poslovnim procesom i koje će spriječiti sukob interesa pri korištenju informacijskog sustava.

10.2 Uprava društva

Uprava Društva je odgovorna za kreiranje poslovne politike Društva i za upravljanje poslovnim procesima, te sigurnosnu politiku.

Uprava Društva može donijeti pravilnike koji detaljnije uređuju pojedine odredbe sigurnosne politike i način korištenja informacijskog sustava.

Uprava Društva može dati nalog za promjenu internih akata o provedbi mjera sigurnosti informacijskog sustava.

10.2.1 Nalog za provedbu mjera sigurnosti

Uprava Društva nadzire provedbu mjera sigurnosti informacijskog sustava.

Uprava Društva služi kao primjer drugim radnicima Društva za provođenje sigurnosnih mjera.

Uprava Društva imenuje nadležne za uvođenje, provedbu i nadzor mjera sigurnosti informacijskog sustava.

Uprava Društva imenuje Glavne korisnike.

10.2.2 Organizacijske mjere sigurnosti informacijskog sustava

Uprava Društva ima obavezu provedbe mjera sigurnosti koje spadaju u područje vođenja Društva ili organizacije rada. Inicijativu za provedbu ovih mjera daju osobe koje su nadležne za mjere sigurnosti informacijskih sustava.

10.2.3 Nadzor nad provedbom mjera sigurnosti informacijskog sustava

Uprava Društva dužna je redovito pratiti razinu sigurnosti informacijskog sustava na način da bude obaviještena o svim odstupanjima od standarda propisanog u dokumentaciji objavljenoj u sustavu kvalitete, o svim težim sigurnosnim prekršajima, te o pojavi sigurnosnih incidenata.

10.3 Sektor upravljanja informacijskim tehnologijama

10.3.1 Nadležnosti za definiciju i nadzor provedbe mjera sigurnosti informacijskog sustava

Voditelj sigurnosti IT sustava, Direktor i voditelji službi Sektora upravljanja informacijskim tehnologijama su nadležni za definiciju i nadzor provedbe mjera sigurnosti informacijskog sustava.

Nadležne osobe određuju i provjeravaju provedbu mjera informatičke sigurnosti u svim organizacijskim dijelovima Društva i na svim dijelovima informacijskog sustava.

Nadležne osobe imaju sljedeće zadatke:

- sudjelovanje u izradi i realizaciji koncepta informacijske sigurnosti
- sudjelovanje u izradi održavanju projektne, korisničke i ostale dokumentacije vezane uz informacijsku sigurnost
- vođenje brige o ukupnoj sigurnosti informacijskih sustava
- sudjelovanje u izradi i provedbi procedura sukladno politici informacijske sigurnosti
- praćenje ostvarenih rezultata sustava kvalitete i sustava sigurnosti
- poticanje definiranja preventivnih i korektivnih mjera u području svoje nadležnosti

10.3.2 Upravljanje rizicima informacijskog sustava

Voditelj sigurnosti IT sustava je odgovoran za provedbu procesa upravljanja rizicima informacijskog sustava.

Voditelj sigurnosti IT sustava i Direktor upravljanja informacijskim tehnologijama izvještavaju Upravu Društva o rezultatima procjene rizika te daju prijedlog Upravi Društva za postupanje u odnosu na utvrđene rizike.

10.3.3 Praćenje i izvještavanje o mjerama sigurnosti informacijskog sustava

Voditelj upravljanja ICT infrastrukturom provodi periodičku provjeru adekvatnosti i primjerenosti mjera informacijskog sustava.

Ukoliko uoči odstupanje od propisanih mjera sigurnosti, onda je Voditelj upravljanja ICT infrastrukturom dužan provesti postupak koji će voditi otklanjanju uočenih nedostataka i otkrivanju uzroka i počinitelja.

U takvim aktivnostima mogu sudjelovati i druge osobe koje predloži Voditelj sigurnosti IT sustava ili Direktor upravljanja informacijskim tehnologijama.

Voditelj sigurnosti IT sustava i Direktor upravljanja informacijskim tehnologijama dužni su izvještavati Upravu Društva o provođenju programa sigurnosti informacijskog sustava, a naročito o svakom slučaju odstupanja od sigurnosne politike ili o sigurnosnim incidentima, vezanim uz informacijski sustav.

10.3.4 Edukacija o mjerama sigurnosti informacijskog sustava

Voditelj sigurnosti IT sustava i Direktor upravljanja informacijskim tehnologijama određuju teme edukacije o informacijskoj sigurnosti te su nadležni za obradu pojedine edukacijske teme i provedbu izobrazbe za sve radnike Društva.

U takvim aktivnostima mogu sudjelovati i druge osobe koje predlože Voditelj sigurnosti IT sustava ili Direktor upravljanja informacijskim tehnologijama.

10.3.5 Proces očuvanja kontinuiteta informacijskog sustava

Voditelj sigurnosti IT sustava i Direktor upravljanja informacijskim tehnologijama trebaju sudjelovati u koordinaciji aktivnosti kojima je za cilj očuvati neprekidnost poslovnih procesa u iznimnim situacijama.

Aktivnosti iz prethodnog stavka uključuju donošenje, implementaciju i provjeru plana djelovanja u slučaju izvanrednih situacije.

U takvim aktivnostima mogu sudjelovati i druge osobe koje predlože Voditelj sigurnosti IT sustava ili Direktor upravljanja informacijskim tehnologijama.

10.3.6 Sudjelovanje u procesu razvoja informacijskog sustava

Voditelj sigurnosti IT sustava i Direktor upravljanja informacijskim tehnologijama sudjeluju u postupku dizajna i razvoja informacijskih sustava s ciljem primjene zahtjeva u pogledu sigurnosti.

U takvim aktivnostima mogu sudjelovati i druge osobe koje predloži Direktor sektora upravljanja informacijskim tehnologijama.

10.3.7 Odgovaranje na sigurnosne incidente

Voditelj sigurnosti IT sustava i Direktor upravljanja informacijskim tehnologijama sudjeluju u provođenju istrage o dojavljenim povredama sigurnosne politike ili o aktivnostima za koje se sumnja da su sigurnosni incidenti.

U slučajevima odgovora na sigurnosne incidente, Voditelj sigurnosti IT sustava i Direktor upravljanja informacijskim tehnologijama dužni su postupiti sukladno internim aktima Društva.

U takvim aktivnostima mogu sudjelovati i druge osobe koje predlože Voditelj sigurnosti IT sustava ili Direktor upravljanja informacijskim tehnologijama.

10.3.8 Druge obaveze

Voditelj sigurnosti IT sustava ima obavezu aktivno pomagati sve radnike Društva u provedbi mjera sigurnosti informacijskog sustava.

Voditelj sigurnosti IT sustava dužan je potaknuti poboljšanja i proširenja u radu službe tehničke potpore korisnicima.

10.4 Glavni korisnici

10.4.1 Polazišta

Nadležnost nad radom pojedinog programskog modula ima organizacijski dio Društva u kojoj je pojedini programski modul najzastupljeniji u poslovnim procesima

Glavni korisnik je osoba odgovorna za kontrolu ispravnosti rada pojedinih programskih modula i za vjerodostojnost podataka koji nastaju unutar ovih programskih modula.

Glavnog korisnika imenuje Uprava Društva, a to je u pravilu rukovoditelj organizacijske cjeline nadležne za rad pojedinog programskog modula.

Sve obaveze Glavnog korisnika se primjenjuju i u slučajevima kada je Pružatelj informatičkih usluga vanjski poslovni subjekt s kojim Društvo ima ugovorni odnos.

Popis Glavnih korisnika i programskih modula nad kojima su Glavni korisnici nadležni nalazi se u dokumentu '*Priručnik o informacijskoj sigurnosti OP-ITM-005*'. Direktori sektora odgovorni su za aplikacije sukladno tablici s popisom Glavnih korisnika, a za zajedničke servise Sektor upravljanja informacijskim tehnologijama.

10.4.2 Odluka o kritičnosti podataka

Glavni korisnik donosi odluku o značaju podataka iz svoje nadležnosti s obzirom na povjerljivost, dostupnost i cjelovitost.

Glavni korisnik sudjeluje s Voditeljem sigurnosti IT sustava u procesu procjene rizika informacijskog sustava.

Glavni korisnik dogovara s Pružateljem informatičkih usluga prihvatljive uvjete korištenja informacijskog sustava, na način da se omogući raspoloživost i cjelovitost sustava, te povjerljivost podataka sukladno zahtjevima poslovnog procesa.

10.4.3 Nadležnost za pristup podacima

Glavni korisnik je dužan identificirati kriterije u odnosu na pristup podacima, što podrazumijeva mogućnosti različitih akcija nad podacima sukladno zahtjevima radnih procesa.

Glavni korisnik može odrediti grupe korisnika sukladno definiranim kriterijima korištenja.

Glavni korisnik može odobriti posebnu proceduru za dodjelu prava pristupa podacima iz svoje nadležnosti.

U slučaju da je Glavni korisnik prenio dio ili ukupne ovlasti za skrb o podacima Pružateljem informatičkih usluga, Glavni korisnik zadržava odgovornost odobravanja korisničkih ovlasti za pristup podacima kako je definirano ovim člankom.

10.4.4 Nadležnost za sigurnost podataka

Glavni korisnik dužan je o svim pitanjima vezanim za sigurnost podataka ili o drugim pitanjima sigurnosti informacijskog sustava konzultirati Voditelja sigurnosti IT sustava.

Glavni korisnik dužan je povremeno provjeravati stanje sigurnosti podataka za koje je odgovoran.

Takva provjera može biti usklađena s postupcima redovite provjere u nadležnosti Uprave Društva, a Glavni korisnik može zahtijevati pomoć za postupak provjere i od Voditelja sigurnosti IT sustava.

Glavni korisnik dužan je prepoznati sve promjene u pogledu sigurnosnih zahtjeva prema podacima za koje je odgovoran.

Glavni korisnik dužan je o takvim zahtjevima izvijestiti Pružatelja informatičkih usluga u razumnom roku, te dati pisani nalog za promjenu sigurnosnih mjera.

10.4.5 Proces očuvanja kontinuiteta poslovanja

Glavni korisnik aktivno surađuje s Voditeljem sigurnosti IT sustava i Direktorom upravljanja informacijskim tehnologijama u postupku planiranja održanja neprekidnosti poslovnih procesa u izvanrednim situacijama.

10.4.6 Prepoznavanje incidenata

Glavni korisnik mora učinite sve što je u njegovoj moći kako bi na vrijeme prepoznao neovlašteni pristup podacima, zloupotrebu podataka ili druge sigurnosne incidente.

O takvim incidentima je dužan izvijestiti Upravu Društva, Voditelja sigurnosti IT sustava ili Direktora upravljanja informacijskim tehnologijama u najkraćem mogućem roku.

10.5 Pružatelj informatičkih usluga

Pružatelj informatičkih usluga je organizacijska cjelina Društva koja vodi brigu o računalnom sustavu i mreži, sistemskom softveru i sistemskim podacima, aplikativnom softveru i odgovarajućim podacima, nad primljenim ulaznim i nad izlaznim podacima koje proizvodi informacijski sustav, nad dokumentacijom, prijenosnim medijima i drugim dijelovima informacijskog sustava koji omogućuju njegov ispravan rad.

Pružatelj informatičkih usluga može biti i vanjski poslovni subjekt s kojim Društvo ima ugovorni odnos.

Odredbe ovog Pravilnika se odnose na nadležnosti i odgovornost internih Pružatelja informatičkih usluga. Nadležnost i odgovornost vanjskih Pružatelja informatičkih usluga uređuje se ugovorom o poslovnoj suradnji.

10.5.1 Organizacijsko ustrojstvo

Organizacijska cjelina Društva koja je nadležna za pružanje informatičkih usluga je Sektor upravljanja informacijskim tehnologijama.

Voditelj sigurnosti IT sustava je odgovoran za pridržavanje odredbi sigurnosne politike unutar Sektora.

Sektor upravljanja informacijskim tehnologijama, u suradnji s Glavnim korisnikom, nadležan je za definiciju sigurnosnih zahtjeva i kontrolu pristupa vanjskih pružatelja informatičkih usluga.

10.5.2 Nadležnost za mjere sigurnosti informacijskog sustava

Pružatelj informatičkih usluga nadležan je za ispravno funkcioniranje svih dijelova informacijskog sustava putem kojih se pristupa informacijskom sustavu, te pomoću kojih se vrši središnja obrada podataka unutar informacijskog sustava.

Pružatelj informatičkih usluga nadležan je za provedbu i administraciju sigurnosnih mjera kojima je svrha održati raspoloživost, pouzdanost i integritet podataka za koje je Pružatelj informatičkih usluga preuzeo odgovornost, a što uključuje, među ostalim, i sljedeće zadatke:

- vođenje zapisa aktivnosti i incidenata koji mogu imati utjecaj na sigurnost informacijskog sustava
- poduzimanje korektivnih i preventivnih mjera; primjena vlastitih i tuđih sigurnosnih iskustava
- organiziranje i implementacija sustava informacijske sigurnosti te kontrola ovlaštenog pristupa pojedinim sustavima vezano za sigurnost informacijskih sustava
- aktivno sudjelovanje u provedbi Politike kvalitete i Politike sigurnosti
- funkcioniranje sustava kvalitete i sustava sigurnosti u području svoje nadležnosti
- pravovremeno provođenje preventivnih i korektivnih mjera u području svoje nadležnosti
- angažiranje na izradi i izmjenama dokumentacije sustava kvalitete i sustava sigurnosti

Aktivnosti i mjere koje provodi Pružatelj informatičkih usluga moraju biti sukladne odredbama sigurnosne politike, odluci o osjetljivosti i kritičnosti podataka koju donosi Glavni korisnik i provedenoj procjeni sigurnosnog rizika.

Glavni korisnik može zatražiti dodatne mjere sigurnosti od onih koje je predvidio Pružatelj informatičkih usluga.

Sigurnosne mjere moraju obuhvaćati osobna računala, mrežne servere, mrežne uređaje i mrežnu infrastrukture informacijskog sustava putem kojih se obavlja pristup informacijskom sustavu, te sistemski i aplikativni softver koji se na takvim resursima koristi.

Poticaj za pokretanje sigurnosnih mjera daju odgovorna osoba i stručno Pružatelj informatičkih usluga, na osnovu odredbi sigurnosne politike, stručnog znanja ili naloga Glavnog korisnika.

Inicijativu iz prethodnog stavka mogu pokrenuti i Voditelj sigurnosti IT sustava i Direktor upravljanja informacijskim tehnologijama.

10.5.3 Dodjela prava pristupa

Davatelj usluga nadležan je za dodjelu prava za pristup podacima za korisnike informacijskog sustava, a na osnovi propisane procedure.

Navedena procedura mora biti dokumentirana i provedena na prema odredbama sigurnosne politike.

10.5.4 Provjera mjera sigurnosti informacijskog sustava

Odgovorna osoba Pružatelja informatičkih usluga dužna je redovito provjeravati stanje sigurnosti informacijskog sustava, s ciljem prepoznavanja i otklanjanja nedostataka, te ukupnog unapređenja sigurnosti informacijskog sustava.

Voditelj sigurnosti IT sustava ima pravo provesti redovit ili povremen nadzor koji mora biti neovisan o postupku drugih osoba Pružatelja informatičkih usluga.

10.6 Korisnici informatičkih usluga

Korisnici mogu pristupati informacijama i koristiti informatičke usluge i resurse samo u skladu s ciljevima kakvi su propisani od Glavnih korisnika i prema sigurnosnoj politici.

Način korištenja informacijskih resursa od korisnika informatičkih usluga opisan je posebnim pravilnicima i pisanim uputama o radu.

Korisnici se moraju pridržavati i drugih uputa koje im može pružati Pružatelj informatičkih usluga, a koje imaju za cilj unaprjeđenje sigurnosti sustava.

11. POŠTIVANJE PRAVILNIKA

Za kršenje odredbi ovog Pravilnika mogu se provesti mjere sukladno odredbama Pravilnika o radu.

Ovaj Pravilnik je stupio na snagu dana 31.03.2023.