0. Povijest promjena dokumenta

Verzija	Datum	Točka	Opis promjene
1.0	30.04.2025.		Inicijalni dokument

1. Uvod

Grupa za sistemsku administraciju (GSA) nema namjeru postavljati ograničenja koja su u suprotnosti s politikom poduzeća odnosno kulturom otvorenosti, povjerenja i neosporenosti. Obveza GSA je pružanje zaštite zaposlenicima, poduzeću i njihovim poslovnim partnerima samo pred nezakonitim ili štetnim namjernim ili nenamjernim aktivnostima od strane pojedinaca.

Svi sustavi povezani s internetom/intranetom/ekstranetom koji između ostalog obuhvaćaju i računalnu strojnu opremu, programsku opremu, operacijske sustave, korisničke račune za elektronsku poštu, pretraživanje stranica i prijenos datoteka spadaju u vlasništvo poduzeća. Spomenuti sustavi se koriste samo u poslovne svrhe poduzeća te služe isključivo njegovim interesima, te strankama i poslovnim partnerima.

Za učinkovitu zaštitu informacija važno je sudjelovanje i potpora svih zaposlenika u poduzeću, ali i svih drugih osoba koje su u kontaktu sa informacijama ili informacijskim sustavima. Odgovornost svakog korisnika informacijskih sustava je upoznavanje sa smjernicama i postupanje u skladu s njima.

2. Namjena

Svrha ove politike je odrediti prihvatljivu primjenu računalne opreme u poduzeću. Pravila su postavljena zato da bi štitila zaposlenike, ali i samo poduzeće. Neodgovarajuća upotreba izlaže poduzeće rizicima kao što su zaraze računalnim virusima, ugrožavanje mrežnih sustava i djelatnosti, te kršenje zakona.

3. Područje primjene

Ova se politika odnosi na sve zaposlenike, ugovornike, savjetnike, privremeno zaposlene i sve ostale zaposlenike poduzeća uključujući osoblje povezano s trećim stranama. Ona se odnosi i na svu opremu koja je u vlasništvu ili u najmu poduzeća.

4. Politika

4.1. Opća upotreba i vlasništvo

Iako je svrha administracije mreže osiguranje razumnog stupnja privatnosti korisnici moraju biti svjesni da su svi podaci koji su kreirani u sustavima poduzeća, vlasništvo istog. Zbog zaštite mreže uprava ne može garantirati povjerljivost informacija pohranjenih na bilo kojem sustavu poduzeća.

Zaposlenici su odgovorni za razumnu i prihvatljivu upotrebu informacijskih sredstava za osobnu upotrebu. U slučaju nejasnoća, zaposlenici se savjetuju sa svojim nadređenima.

U svrhu upravljanja sigurnošću mrežama, ovlaštene osobe bilo kada mogu izvoditi nadzor nad opremom, sustavima i protokom podataka u skladu sa politikom kontrole informacijskih sustava. Poduzeće zadržava pravo periodičnog kontroliranja mreža i sustava sa ciljem osiguranja usklađenosti s tom politikom.

Za iznošenje opreme, informacija, ili softvera, bez obzira u kojem obliku ili na kojem se mediju nalaze, potrebna je prethodna dozvola izdana putem e-maila i evidentirana kroz sustav Jira od strane direktora ili Administratora sustava.
Dok se navedeni resursi nalaze izvan poduzeća, cijelo vrijeme moraju biti pod kontrolom osobe koja je dobila dozvolu za njihovo iznošenje.
Prilikom prestanka ugovora o radu ili drugog ugovora temeljem kojeg korisnik koristi raznu opremu, softver, ili informacije u elektroničkom ili papirnatom obliku, korisnik je dužan vratiti sve takve informacijske resurse.

4.2. Sigurnost i vlasništvo informacija

Korisničko sučelje mora na internet/intranet/ekstranet sustavima u skladu s politikom poduzeća upozoriti na stupanj povjerljivosti informacija kojima korisnik pristupa. Primjeri povjerljivih informacija su: poslovne tajne, popisi poslovnih partnera, dokumenti o strategijama poduzeća, i podaci o razvojnim projektima. Zaposlenici moraju provoditi sve potrebne mjere kako bi se spriječio neovlašteni pristup povjerljivim informacijama.

Zaporke moraju biti zaštićene, korisnički računi se ne smiju dijeliti s drugima. Korisnici su odgovorni za zaštitu svojih zaporki i korisničkih računa.

Antivirusna zaštita ne može biti isključena.

4.3. Neprihvatljiva upotreba

Zaposlenici se mogu izuzeti od ograničenja ako to zahtijevaju njihove radne obaveze. Niti u jednom slučaju zaposlenici nemaju ovlaštenje za izvođenje nezakonitih radnji dok upotrebljavaju sredstva koja su vlasništvo poduzeća.

Sljedeći popis nije potpun već samo predstavlja okvir za aktivnosti koje nisu dozvoljene.

4.3.1. Aktivnosti u vezi sa sustavima i mrežom

- Kršenje prava bilo koje osobe ili poduzeća koje su zaštićene autorskim pravima, poslovnom tajnom, patentom ili drugim oblikom zaštite intelektualnog vlasništva, uključujući instalaciju i širenje nelegalnih kopija programske opreme.
- Neovlašteno kopiranje i širenje autorskih djela, uključujući digitalizaciju fotografija iz časopisa, knjiga i ostalih izvora te instaliranje bilo koje autorski zaštićene programske opreme za koju pojedinac ili poduzeće nema odgovarajuću licencu.
- Izvoz programske opreme, tehničkih informacija, šifriranih metoda ili tehnologije u druge države u suprotnosti s međunarodnim ili lokalnim zakonima. Prije izvoza potrebno je savjetovanje s odgovornima u poduzeću.
- Instalacija štetne programske opreme na mrežu ili servere (npr. viruse, crve, trojanske konje, e-mail bombe itd.)

- Otkrivanje zaporke korisničkog računa ili omogućavanje upotrebe vlastitog korisničkog računa drugim osobama uključujući članove obitelji i ukućane ako se posao obavlja iz vlastitog doma.
- Upotreba informacijskih sredstava za aktivno sudjelovanje u prikupljanju i širenju materijala povezanih sa spolnim zlostavljanjem ili zlostavljanjem na radnom mjestu (s obzirom na lokalno zakonodavstvo).
- Širenje lažnih ponuda za robu i usluge preko informacijskog sustava poduzeća.
- Davanje izjava o garancijama, eksplicitno ili implicitno ukoliko to nije dio normalnih radnih procedura.
- Izvođenje upada i ometanja mrežnih komunikacija. Upadi pored ostalog uključuju i pristup podacima na koje pojedinac nema pravo ili prijavljivanje na server ili korisnički račun za koje nije ovlašten. Izuzete su slične aktivnosti po službenoj dužnosti. Kako bi razlikovali ova dva slučaja, ometanje pored ostalog predstavlja i presretanje podataka, prijevare s paketima podataka, razni DDoS napadi s namjerom da se nekoga ošteti.
- Skeniranje portova ili zaštite je izričito zabranjeno osim ako se prethodno ne najavi službi za informacijsku sigurnost.
- Izvođenje bilo kakvog nadziranja koje može dovesti do presretanja paketa koji nisu namijenjeni korisnikovom uređaju. Izuzeto je nadziranje po službenoj dužnosti.
- Izbjegavanje autentifikacije ili drugih sigurnosnih mehanizama na bilo kojem serveru, mreži ili korisničkom računu.
- Ometanje ili onemogućavanje djelatnosti bilo kojem korisniku (napad onemogućavanjem djelatnosti).
- Upotreba bilo kojih programa/programskih datoteka/naredbi ili slanja obavijesti bilo koje vrste s namjerom ometanja ili onemogućavanja korisničkih sjednica na bilo kakav način, lokalno ili preko Internet/Intranet/ekstranet mreže.
- Posredovanje informacija ili popisa o zaposlenicima trećim osobama.
- Korištenje uslužnih programa koji mogu nadjačati kontrole sustava i aplikacija.
- Instalacija softvera na operativnim sustavima u vlasništvu poduzeća bez odobrenja GSA.

4.3.2. Aktivnosti u vezi s e-mailom i komunikacijama

- Slanje neželjene e-pošte zajedno sa slanjem spam-a ili drugog reklamnog materijala pojedincima koji nisu dali eksplicitnu suglasnost za primanje takvih obavijesti.
- Sve oblike maltretiranja e-poštom, telefonom ili osobnim pozivom, riječima, frekvencijom ili veličinom poruke.
- Neovlaštena upotreba i krivotvorenje glave e-pošte.
- Zahtijevanje e-poruka za bilo koju adresu osim vlastite u svrhu nanošenja štete i/ili zarade.
- Stvaranje ili posredovanje u slanju lančanih pisama, piramidalnih shema bilo koje vrste.
- Slanje neželjene pošte s mreže poduzeća ili drugih internet/intranet/ekstranet ponuđača djelatnosti u imenu poduzeća ili namjera oglašavanja djelatnosti na mreži poduzeća ili djelatnosti povezanih preko mreža poduzeća.
- Slanje jednakih ili sličnih obavijesti na veći broj news grupa.

5. Poštivanje politike

Za kršenje ove politike primjenjuju se disciplinske mjere propisane internim aktima.

	Ime i prezime:	Funkcija:	Datum:	Potpis:
Odobrio:	Luka Šikić	Direktor	30.04.2025.