OIV Digitalni signali i mreže

ISMS-ZAP-009
SIGURNOSNE UPUTE ZA DOBAVLJAČE I VANJSKE SURADNIKE

Verzija:	1.0
Stupanj povjerljivosti:	OIV_JAVNO
Datum objave:	25. 05. 2022.

Popis kratica / Naziva	Opis
Dobavljač	Pravna ili fizička osoba koja stupa u ugovorni odnos s Društvom tijekom kojeg : • pribavlja robe, materijale, energente i druge resurse potrebne za funkcioniranje i održavanje informacijskih sustava; • pruža vanjske usluge poput razvoja i održavanja informacijskih sustava te izvođenja radova
Društvo	Odašiljači i veze d.o.o.
Dostupnost	Svojstvo informacije koje osigurava da informaciji mogu pristupiti ovlaštene osobe u trenutku kada je informacija potrebna (*engl. Availability*)
HTTPS	*HyperText Transfer Protocol Secure* je internetski protokol nastao kombinacijom protokola HTTP s protokolom SSL/TLS
Informacija	Podatak ili skup podataka s pripisanim značenjem koji, kao osnovni element komunikacije, primljen u određenoj situaciji, povećava korisnikovo znanje
Informacijski sustav	Bilo koji uređaj ili grupa povezanih ili srodnih uređaja, od kojih jedan ili više njih programski izvršava automatsku obradu informacija
Incident informacijske sigurnosti	Pojedinačni događaj ili niz neželjenih ili neočekivanih događaja povezanih s informacijskom sigurnošću kod kojih postoji značajna vjerojatnost da će ugroziti poslovanje i zaprijetiti informacijskoj sigurnosti
Integritet	Svojstvo informacije koje osigurava da informaciju mogu mijenjati samo ovlaštene osobe ili sustavi na dozvoljen način (*engl: Integrity*)
IT	Organizacijska jedinica nadležna za jezgrene mreže, IT i usluge
IT uređaj	IT hardver koji može biti samostalan ili predstavljati sastavni dio informacijskog sustava

Korisnik	Svaka osoba koja koristi informacijski sustav u vlasništvu Društva ili sustave koje Društvo upotrebljava u poslovne svrhe temeljem važećih ugovora
Poslovni vlasnik informacije	Voditelj organizacijske jedinice koji je odgovoran za informacije sadržane u informacijskom sustavu
Povjerljivost	Svojstvo informacije koje osigurava da je informacija dostupna samo ovlaštenim osobama, sustavima, procesima (*engl: Confidentiality*)
SFTP	*Secure File Transfer Protocol*
SSH	*Secure Shell Protocol*
Vanjski suradnik	Osoba koja nije zaposlenik Društva, a zaključuje ugovore bilo koje vrste osim ugovora o nabavi i prodajnih ugovora (npr. ugovor o djelu ili autorskopravni ugovor)

Sadržaj

1. Svrha

Svi dobavljači i vanjski suradnici moraju razumjeti da jedna kriva odluka, jedan krivi klik mišem ili jedan trenutak nemara može dovesti do incidenta informacijske sigurnosti. Incidenti informacijske sigurnosti mogu negativno utjecati na interese Društva poput sukladnosti s regulatornim zahtjevima (npr. pravni postupci uslijed grubog nepoštivanja regulatornih zahtjeva), ispunjenja zadataka (npr. nemogućnost izvođenja ugovorenih zadataka uslijed nedostupnosti kritičnih sustava), narušavanja reputacije (npr. hakerski napadi mogu rezultirati otkrivanjem povjerljivih informacija i negativnim medijskim napisima), negativnih financijskih tokova (npr. visoki penali uslijed povrede podataka, gubitak prihoda uslijed nedostupnosti kritičnih usluga).

2. Područje primjene

Sigurnosne upute za dobavljače i vanjske suradnike definiraju zahtjeve informacijske sigurnosti za sve dobavljače i vanjske suradnike s kojima Društvo stupa u ugovorni odnos i razmjenjuje povjerljive ili osobne informacije. Postizanjem sukladnosti sa sigurnosnim zahtjevima, dobavljač ili vanjski suradnik razumije sigurnosne upute i upoznat je s načinom kako upravljati informacijama, računalnom opremom i informacijskim sustavima na siguran način i kako se prikladno ponašati za vrijeme suradnje s Društvom.

Ove upute se odnose na sve dobavljače i vanjske suradnike Društva. Svi dobavljači i vanjski suradnici moraju biti usklađeni sa zahtjevima informacijske sigurnosti za vrijeme upravljanja informacijama, računalnom opremom i/ili informacijskim sustavima Društva.

Sigurnosni zahtjevi su primjenjivi na informacije Društva, kao i sve potporne informacijske sustave kojima Dobavljač ili vanjski suradnik upravlja prilikom obrade informacija.

Pojedinosti navedene u ovom dokumentu zamišljene su kao minimalni obavezni sigurnosni zahtjevi za dobavljače i vanjske suradnike Društva u skladu s Politikom informacijske sigurnosti.

3. Zahtjevi informacijske sigurnosti za dobavljače i vanjske suradnike

3.1. Opći zahtjevi

Svim informacijama, računalnom opremom (npr. prijenosna računala, stolna računala, pametni telefoni, USB, CD/DVD) treba rukovati s pažnjom dobrog vlasnika. Informacije se ne smiju slati na privatne e-mail adrese, pohranjivati na privatne resurse, slati na javne cloud usluge ili na druge servise koji nisu odobreni od strane Društva ili opisani ugovorom. Dobavljač ili vanjski suradnik će se suzdržati od svih aktivnosti koje mogu negativno utjecati na informacije Društva ili informacijske sustave Društva, poput sljedećih aktivnosti (ali nije ograničeno na):

- pristup, preuzimanje ili distribucija: nelegalnom sadržaju, nasilnom sadržaju, diskriminatornom sadržaju, pornografskom sadržaju, reklamnom sadržaju, lančanim e-mail porukama, sumnjivim i malicioznim e-mail porukama koje sadrže nepoznate poveznice ili sumnjive priloge, ili poruke koje imitiraju menadžment s uputama za prijenos novca
- kršenje zakona i ostale regulative, kršenja prava na intelektualno vlasništvo ili licenčnih prava
- kockanje i rudarenje kripto valuta (npr. Bitcoin, Ethereum)

- aktivnosti koje mogu rezultirati uskraćivanjem pružanja usluga ili prekida poslovanja
- zaobilaženje sigurnosnih kontrola

Dobavljač ili vanjski suradnik ograničit će upotrebu nesigurnih komunikacijskih protokola, upotreba sigurnih i aktualnih komunikacijskih protokola (npr. SSH, HTTPS, SFTP) kada se komunikacija odvija putem javnih mreža, uključujući i internet.

Alarmi i upozorenja o kojima obavještavaju organizacijske jedinice nadležne za sigurnost i IT bit će shvaćeni ozbiljno, a dobavljač ili vanjski suradnik postupit će prikladno po primitku upozorenja.

3.2. Obaveze uporabe korisničkih računa

Svakom dobavljaču i vanjskom suradniku s pristupom informacijskim sustavima Društva dodijeljen je korisnički račun. Svi dobavljači i vanjski suradnici štitit će svoje korisničke račune u svrhu sprečavanja zlouporabe.

Navedeno uključuje sljedeće (ali nije ograničeno na):

- dobavljač ili vanjski suradnik neće dijeliti korisničke račune
- u slučaju sumnje u kompromitaciju korisničkog računa o istom je odmah potrebno obavijestiti kontakt osobu Društva ili putem dogovorenih kanala IT Društva

3.3. Odabir i uporaba lozinki

Svi dobavljači i vanjski suradnici osigurat će upotrebu jakih lozinki. Predloženi minimalni zahtjevi za odabirom jake zaporke su:

- minimalna dužina od 8 znakova
- barem jedno veliko slovo, jedno malo slovo, jedan broj i jedan specijalni znak
- upotreba osobnih podataka (npr. ime, rođendan, broj zaposlenika) je zabranjeno
- uzroci na tipkovnici (npr. asdf, 1234) kao i riječi iz rječnika nije preporučljivo koristiti

Lozinke moraju ostati tajne. U slučaju sumnje u kompromitaciju lozinke istu je odmah potrebno promijeniti i o događaju obavijestiti kontakt osobu Društva putem dogovorenih kanala IT Društva.

Dozvoljeno je korištenje sigurnosnih fraza (engl: *passphrase*), uz poštivanje pravila definiranih za lozinke sigurnosne fraze moraju sadržavati najmanje 15 znakova.

3.4. Klasifikacija informacija

Dobavljači i vanjski suradnici osigurat će prikladno upravljanje informacijama na niže opisani način.

Stupanj povjerljivosti	**JAVNO**
Fiz. i admin. kontrola	Nema
Umnožavanje	Neograničeno
Pohrana	Bez ograničenja

Distribucija	Bez ograničenja
Uništavanje/zbrinjavanje	Recikliranje/smeće
Odobrenje za otkrivanje trećim stranama daje:	Nije potrebno

Stupanj povjerljivosti	**INTERNO**
Fiz. i admin kontrola	• **Poslovni vlasnik informacije:** odgovoran za pravilno označavanje • **Korisnik:** odgovoran za pravilnu pohranu, obradu, distribuciju, umnožavanje, uništavanje i nadzor dokumenata
Umnožavanje	Kopirati u ograničenoj mjeri smiju samo zaposlenici, dobavljači i vanjski suradnici s kojima su potpisani odgovarajući sporazumi o povjerljivosti
Pohrana	• **U papirnatom obliku**: držati zaključano kada se ne koristi • **U elektroničkom obliku**: samo na resursima koje na raspolaganje stavi ili ih odobri IT
Distribucija	• **Interno**: koristite omotnicu za dostavu interne pošte • **Eksterno**: koristite zatvorenu omotnicu • **U elektroničkom obliku**: Kada je riječ o slanju na interne i eksterne adrese e-pošte potrebno je obratiti posebnu pozornost prilikom upisa adrese primatelja • **Putem telefaksa**: provjerite broj telefaksa
Uništavanje/zbrinjavanje	• **Dokumenti u papirnatom obliku**: usitnite strojno i odložite u spremnik papir • **Podaci u elektroničkom obliku**: obrišite podatke
Odobrenje za otkrivanje trećim stranama daje:	Poslovni vlasnik informacije

Stupanj povjerljivosti	**POVJERLJIVO**
Fiz. i admin. kontrola	• **Poslovni vlasnik informacije:** odgovoran za pravilno označavanje • **Korisnik**: odgovoran za pravilnu pohranu, obradu, distribuciju, umnožavanje, uništavanje i nadzor dokumenata
Umnožavanje	Kopirati u ograničenoj mjeri smiju samo zaposlenici, dobavljači i vanjski suradnici s kojima su potpisani odgovarajući sporazumi o povjerljivosti
Pohrana	• **U papirnatom obliku:** držati zaključano kada se ne koristi • **U elektroničkom obliku:** samo na resursima zaštićenim zaporkom koje odobri IT

Distribucija	• **Interno:** koristite omotnicu za dostavu interne pošte • **Eksterno:** koristite zatvorenu omotnicu. Isporuka osobno ili slanje preporučenom poštom, putem kurirske službe i sl. • **Elektronički - interno:** Za slanje na interne adrese e-pošte preporučuje se zaštita podataka šifriranjem. Ukoliko se koristi, zaporka mora biti dostavljena putem drugog komunikacijskog kanala • **Elektronički - eksterno:** Kod slanja na vanjske adrese e-pošte zahtijeva se zaštita podataka šifriranjem. Ukoliko se koristi, zaporka mora biti dostavljena putem drugog komunikacijskog kanala • **Putem telefaksa:** provjerite broj telefaksa
Uništavanje/zbrinjavanje	• **Dokumenti u papirnatom obliku:** usitnite strojno ili odlaganjem u spremnik za sigurno uništavanje papira • **Elektronički podaci:** sigurnosno brisanje, kontaktirajte IT za potporu
Odobrenje za otkrivanje trećim stranama daje:	Poslovni vlasnik informacije

Stupanj povjerljivosti	**TAJNO**
Fiz. i admin. kontrola	• **Poslovni vlasnik informacije**: odgovoran je za odgovarajuće označavanje te je dužan pobrinuti se za to da se strogo povjerljive informacije distribuiraju strogo u skladu s načelom pristupa informacijama nužnim za obavljanje poslovnih obveza • **Korisnik**: odgovoran je za kriptiranje strogo povjerljivih informacija i/ili je dužan pobrinuti se da su, u vrijeme kada se ne koriste, strogo povjerljive informacije pod ključem
Umnožavanje	Moguća je izrada ograničenog broja kopija uz poslovnog vlasnika informacija, odnosno osoba koje je on odredio.
Pohrana	• **U papirnatom obliku**: držati zaključano kada se ne koristi • **U elektroničkom obliku**: samo na resursima koji su zaštićeni zaporkom, koje odobri IT
Distribucija	• **Interno**: koristite zapečaćenu omotnicu. Po mogućnosti isporučiti osobno • **Eksterno**: koristite zapečaćenu omotnicu. Isporuka osobno ili slanje preporučenom poštom, putem kurirske službe i sl. • **U elektroničkom obliku**: Za slanje na unutarnje i vanjske adrese e-pošte obavezna je zaštita podataka šifriranjem. Ukoliko se koristi, zaporka mora biti dostavljena putem drugog komunikacijskog kanala. • **Slanje putem telefaksa**: neposredno prije slanja informacija telefaksom obavezna je telefonska potvrda primitka testne stranice te je također potrebna telefonska potvrda primitka svih dokumenata

Uništavanje/zbrinjavanje	• **Dokumenti u papirnatom obliku:** strojno usitnjavanje • **Elektronički podaci**: sigurnosno brisanje. Kontaktirajte IT za potporu.
Odobrenje za otkrivanje trećim stranama daje:	Uprava Društva

Sve informacije koje nisu izričito klasificirane i sve informacije koje sadrže osobne podatke moraju se tretirati kao informacije klasificirane "Povjerljivo".

Sve informacije stupnja povjerljivosti “Interno“, “Povjerljivo“ i „Tajno“ smatraju se Poslovnom tajnom.

3.5. Politika praznog stola i ekrana

- Prilikom napuštanja radnoga stola korisnici se moraju pobrinuti da zaslon računala bude zaključan, odnosno moraju se odjaviti iz sustava i zaključati pametni telefon. Automatsko zaključavanje ekrana je potrebno postaviti na maksimalno 10 minuta neaktivnosti.
- na kraju radnog dana, potrebno je odjaviti se ili zaključati uređaje
- Informacije klasificirane "Interno", "Povjerljivo" i "Tajno" ne smiju biti odložene na stolu u odsustvu korisnika. Informacije je potrebno zaključati u ladice ili ormare
- lozinke, PIN-ovi ili ostale personalizirane informacije zabranjeno je zapisivati i ostavljati na vidljivim lokacijama
- potrebno je osigurati da se tiskane informacije klasificirane "Interno", "Povjerljivo" i "Tajno" ne ostavljaju na uređajima za tiskanje
- ploče za pisanje ili ostali mehanizmi vizualizacije na kojima su zapisane informacije klasificirane "Interno", "Povjerljivo" i "Tajno" potrebno je očistiti nakon upotrebe
- Informacije, posebno dokumenti i oprema koja se upotrebljava na sastancima, uklonit će se nakon što sastanak završi. Informacije koje više korisnici ne trebaju bit će uništene.

3.6. IT uređaji koji obrađuju informacije Društva

- IT uređaji bit će opremljeni operativnim sustavom koji je ažuriran u skladu s uputama proizvođača
- antivirusna rješenja potrebno je instalirati na korisničke uređaje
- IT uređaj potrebno je zaštiti pristupnim kontrolama
- IT uređaj potrebno je zaštititi od neovlaštene uporabe
- IT uređaj neće biti dan neovlaštenim osobama (uključuje obitelj)
- o upotrebi informacijskih sustava potrebno je voditi zapise (logove) u svrhu osiguranja odgovornosti i neporecivosti
- sigurnosni zapisi bit će zaštićeni od neovlaštene izmjene ili brisanja

3.7. Korištenje informacijske imovine Društva u privatne svrhe

- sve informacije, imovina ili usluge u vlasništvu Društva bit će upotrebljavane isključivo u poslovne svrhe

- Pohrana privatnih podataka na resurse Društva je zabranjena. Društvo može obrisati sve privatne informacije pohranjene na resurse Društva bez prethodnog obavještavanja korisnika.
- dobavljači i vanjski suradnici svjesni su da sve što rade na informacijskim sustavima Društva može se retroaktivno otkriti i istražiti u slučaju sumnje u neprikladnu upotrebu

3.8. Pohrana poslovnih informacija

- dobavljači i vanjski suradnici pohranjivat će informacije Društva na svoju IT opremu u skladu s uputama opisanih ovim dokumentom
- poslovne informacije zabranjeno je pohranjivati na javnim servisima računarstva u oblaku koji nisu odobreni od strane nadležnih organizacijskih jedinica dobavljača ili vanjskih suradnika
- sve informacije potrebno je pohraniti na siguran način i osigurati od neovlaštenog pristupa u skladu s klasifikacijom informacija

3.9. Iznošenje opreme i informacija

- informacije i IT uređaji se ne smiju kopirati ili iznositi iz ureda bez jasne dozvole poslovnog vlasnika informacija
- dobavljači i vanjski suradnici osigurat će sve potrebne mjere na javnim mjestima kojima se sprečava otkrivanje povjerljivosti informacija

3.10. Komunikacija

- dobavljači i vanjski suradnici će s dužnom pažnjom zaštiti komunikaciju od neovlaštenog pristupa ili prisluškivanja
- dobavljači i vanjski suradnici upotrebljavat će VPN komunikaciju za pristup infrastrukturi Društva
- isključivo sigurni komunikacijski protokoli upotrebljavat će se za prijenos informacija u skladu s klasifikacijom informacija.

3.11. Izvještavanje o nastalim incidentima informacijske sigurnosti

- dobavljači i vanjski suradnici izvijestit će društvo o nastalim sigurnosnom incidentima putem odgovorne osobe u Društvu ili direktno putem elektroničke pošte na adresu: noc@oiv.hr ili telefonom na +385 1 6186 666 ili +385 1 6186 667
- dobavljači i vanjski suradnici pružit će nužnu potporu u analizi i korekciji incidenta