# **PRAVILNIK O SUSTAVU INFORMACIJSKE SIGURNOSTI**

|  |  |  |  |
| --- | --- | --- | --- |
| **Naziv** | Pravilnik o sustavu informacijske sigurnosti | | |
| **Datum** | ${psis\_01} | **Verzija** | 1.0 |

Voditelj obrade: ${psis \_02\_a}

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Potpis ovlaštene osobe za zastupanje

1. Svrha

Ovim pravilnikom o sustavu informacijske sigurnosti **(„Pravilnik“)** uređuju se mjere i postupci koji služe za prevenciju od gubitka ili neovlaštenog otkrivanja te se uređuje otkrivanje i otklanjanje posljedica u slučaju gubitka ili neovlaštenog otkrivanja osobnih podataka koje obrađuje voditelj obrade ${psis \_02\_b} („**Organizacija**“), kao i službenih podataka Organizacije.

1. Definicije

Sve definicije u ovom Pravilniku pisane velikim početnim slovom (npr. Osobni podatak) imaju isto značenje kao što je definirano u ostalim internim aktima Organizacije, osim ako što drugo nije izričito određeno i definirano u ovom Pravilniku.

Pojmovi navedeni u ovom Pravilniku velikim početnim slovom imaju sljedeće značenje:

**Službeni podatak**: dokument, odnosno svaki napisani, umnoženi, nacrtani, slikovni, tiskani, snimljeni, fotografirani, magnetni, optički, elektronički ili bilo koji drugi zapis podatka, saznanje, mjera, postupak, predmet, usmeno priopćenje ili informacija, koja s obzirom na svoj sadržaj ima važnost povjerljivosti i cjelovitosti za Organizaciju, a osobito poslovne tajne i Osobni podaci, podaci o sklopljenim ugovorima i bitnim sastojcima ugovora, o uvjetima pružanja usluga od strane Organizacije, *know-how* Organizacije, i sl.

**Informacijski sustav**: računalni, komunikacijski ili drugi elektronički sustav u kojem se Službeni podaci obrađuju, pohranjuju ili prenose tako da budu dostupni i uporabljivi za Ovlaštene osobe, a koji obuhvaća tehničku infrastrukturu, organizaciju, osobe i postupke kojima se podaci obrađuju, pohranjuju ili prenose.

**Pristup:** svaka radnja koja uključuje mogućnost uvida, preuzimanja, otkrivanja, izmjene ili brisanja podataka

**Mjere sigurnosti**: skup mjera i postupaka, na tehničkoj i organizacijskoj razini, čijom se primjenom postiže i održava prihvatljiva razina zaštite sigurnosti Informacijskog sustava.

**Sigurnosni incident**: događaj koji ugrožava povjerljivost, integritet i dostupnost Službenih podataka, integritet i sigurnost Informacijskog sustava, ili ukazuje na neovlašteni pristup Informacijskom sustavu.

1. Primjena Pravilnika

Ovaj Pravilnik obvezuje sve zaposlenike (Ovlaštene osobe) i vanjske suradnike Organizacije kojima je dozvoljen pristup Informacijskom sustavu.

Vanjskim suradnicima Organizacije, po potrebi, se mogu dodijeliti prava Ovlaštene osobe, s tim da se i u odnosu na njih primjenjuju odredbe ovog Pravilnika.

Kršenje odredbi ovog Pravilnika od strane Ovlaštenih osoba može dovesti do izvanrednog otkaza ugovora o radu, a u slučaju kršenja od strane Vanjskih suradnika Organizacije do raskida ugovornog odnosa.

1. Prava i obveze Ovlaštenih osoba

Ovlaštene osobe određuje odgovorna osoba unutar Organizacije, a Ovlaštene osobe određuju se s obzirom na radno mjesto i sukladno poslovnim procesima koje obavljaju te se s tim u vezi određuje i opseg ovlasti za pristup Informacijskom sustavu u skladu s potrebama njihovog radnog mjesta.

Opseg ovlasti za pristup Informacijskom sustavu koje su dodijeljene Ovlaštenoj osobi ne smije prelaziti ovlasti koje Ovlaštena osoba ima u redovitom poslovnom procesu.

Ovlaštene osobe dužne su se pridržavati odredbi ovog Pravilnika radi osiguranja pravilnog rada i zaštite sigurnosti Informacijskog sustava te sprječavanja Sigurnosnih incidenata.

Ovlaštene osobe dužne su poduzimati sve mjere sigurnosti propisane ovim Pravilnikom kao i druge razumne mjere sigurnosti radi osiguranja pravilnog rada i zaštite sigurnosti Informacijskog sustava i sprječavanja Sigurnosnih incidenata odnosno njihova otklanjanja.

1. Zaštita Informacijskog sustava

**5.1. Kontrola i zaštita pristupa**

Odgovorna osoba unutar Organizacije dodjeljuje prava za pristup informacijskom sustavu Ovlaštenim osobama sukladno potrebama njihovog radnog mjesta i to u najmanjoj mjeri potrebnoj za obavljanje radnih zadataka u okviru redovitog poslovnog procesa.

Odgovorna osoba unutar Organizacije vodi evidenciju odobrenja pristupa te istu evidenciju i dodijeljene ovlasti revidira uslijed svake značajnije promjene u sustavu, a najmanje jednom godišnje.

Ovlaštene osobe prilikom pristupa informacijskom sustavu identificiraju se korištenjem korisničkog imena i lozinke, a Ovlaštene osobe odgovorne su za izbor i čuvanje tajnosti lozinki koje koriste.

Pri odabiru lozinke Ovlaštena osoba mora voditi računa da koristi snažnu lozinku koju redovito mijenja (najmanje jedanput godišnje), a koja treba sadržavati najmanje 12 znakova te treba sadržavati jedno ili više od sljedećeg: velika slova (ABCDE...), mala slova (abcde...), brojke (0-9), simbole (@#$%{ } [ ] ( ) / \ ' " , ; : . < >…), interpunkcijske znakove (?, ", !).

Ovlaštena osoba je dužna čuvati tajnost lozinke i ne odavati je drugim osobama. Iznimno, ako nastane opravdana potreba za pristupom određenom dijelu Informacijskog sustava od strane druge Ovlaštene osobe, a tom dijelu se može pristupiti isključivo putem lozinke Ovlaštene osobe, Ovlaštena osoba može odati lozinku drugoj Ovlaštenoj osobi. U takvom slučaju, Ovlaštena osoba koja je odala lozinku dužna je zamijeniti lozinku bez odgađanja u najkraćem mogućem roku.

U slučaju više sile ili odsutnosti s radnog mjesta, Ovlaštena osoba, uz, ako je primjenjivo, savjet osobe koja je zadužena za zaštitu osobnih podataka u Organizaciji, koja je administrator sustava može radi uvida u Službene podatke izvršiti uvid u Informacijski sustav Organizacije. Takav uvid se obavlja samo u odnosu na Službene podatke te podatke koji su nužni radi ostvarivanja uvida (npr. dogovor s poslovnim suradnikom oko proizvoda i usluge, dogovorene cijene i datumi) te se nakon uvida izrađuje zapisnik o pristupu.

**5.2. Pravila korištenja opreme**

Oprema Organizacije smije se koristiti isključivo u poslovne svrhe, a sva oprema mora biti evidentirana i svi korisnici opreme zabilježeni.

Oprema Organizacije ne smije se koristiti u privatne svrhe, osim uz izričito dopuštenje Organizacije.

Korištenje opreme Organizacije, odnosno osobne opreme koja se koristi u poslovne svrhe, mora biti u skladu sa zakonom, internim aktima Organizacije i licencnim pravima.

Oprema Organizacije mora biti zaštićena na adekvatan način (antivirusna zaštita), primjeren određenoj vrsti opreme Organizacije.

Ovlaštene osobe su odgovorne za profesionalno, etično i zakonito korištenje opreme Organizacije i osobne opreme kada se koristi za poslovne svrhe.

Oprema Organizacije, odnosno osobna oprema kada se koristi u poslovne svrhe mora, ako je to tehnički moguće i ne zahtijeva nerazmjeran napor, biti zaštićena odgovarajućom složenom lozinkom ili na drugi način koji onemogućava izravan pristup toj opremi od strane trećih osoba koje nisu Ovlaštene osobe.

Ovlaštene osobe su dužne mijenjati lozinke za pristup opremi Organizacije, odnosno osobnoj opremi koja se koristi u poslovne svrhe, najmanje jedan put godišnje.

Ovlaštene osobe su dužne poduzeti sve potrebne Mjere sigurnosti kako bi spriječile otuđenje korporativne opreme, odnosno osobne opreme koja se koristi u poslovne svrhe.

Ovlaštene osobe ne smiju davati opremu Organizacije na uporabu trećim osobama, a u slučaju davanja osobne opreme koja se koristi u poslovne svrhe moraju poduzeti sve razumne Mjere sigurnosti kako bi spriječili nastanak Sigurnosnog incidenta.

## **5.3. Pravila korištenja osobne opreme**

Korištenje osobne opreme u poslovne svrhe predstavlja rizik za poslovanje, u najvećoj mjeri prisutan kao rizik od neovlaštenog pristupa, krađe i gubitka podataka.

Dozvoljeno je spajanje vlastitih uređaja za pohranu podataka (npr. eksterni diskovi) na opremi Organizacije u svrhu izrade sigurnosnih kopija podataka, te prijenosa podataka u slučaju da to nije moguće ili nije dovoljno praktično odraditi preko Informacijskog sustava. Prije korištenja vlastitog uređaja za pohranu podataka potrebno je provjeriti uređaj i njegov sadržaj antivirusnim alatom. Nije dozvoljeno spajanje i korištenje uređaja koji su zaraženi virusima ili drugim zlonamjernim programima. Ako se uređaj za pohranu podataka iznosi izvan prostorija Organizacije, Službeni i Osobni podaci na uređaju moraju biti šifrirani, te dodatno zaštićeni lozinkom za pristup uređaju, ako uređaj ima tu mogućnost. Kada više nisu potrebni svi podaci moraju biti obrisani na siguran način.

Nije dozvoljeno kopiranje i spremanje internih i povjerljivih podataka na vlastite uređaje bez prethodnog odobrenja Organizacije. Na vlastite uređaje i medije za pohranu podataka nije dozvoljeno kopiranje i spremanje podataka koji su označeni kao poslovna tajna, čak niti u šifriranom obliku.

## **5.4. Korištenje službenih informacijskih sustava i elektroničke pošte**

Ovlaštene osobe dužne su koristiti službene informacijske sustave Organizacije i službenu elektroničku poštu Organizacije na takav način kojim se izbjegava nanošenje štete Organizaciji te nastanak Sigurnosnog incidenta.

Sadržaj koji se šalje putem službene elektroničke pošte mora biti pisan pažljivo i odmjereno kako bi se izbjegao nastanak Sigurnosnog incidenta.

Servis elektroničke pošte smije se koristiti isključivo za službenu komunikaciju. Zabranjeno je slanje elektroničke pošte sa službene adrese elektroničke pošte u privatne svrhe.

Poruke na službenom servisu elektroničke pošte smatraju se službenim dokumentima.

Nije dopušteno automatski prosljeđivati poruke elektroničke pošte na drugi korisnički račun, odnosno bilo koju drugu adresu elektroničke pošte koja ne pripada Organizaciji, bez dopuštenja uprave Organizacije.

Pri prestanku radnog ili drugog ugovornog odnosa, Ovlaštena osoba informatičke podrške Organizacije mora osigurati zatvaranje korisničkog računa Ovlaštene osobe, na način da se sa zadnjim danom deaktivira korisnički račun i šalje automatska elektronička poruka pošiljateljima kome se mogu obratiti, a potom se nakon 2 mjeseca korisnički računi brišu.

## **5.5. Pristup internetu i korištenje internetskih usluga**

Internet se može koristiti isključivo za poslovnu namjenu, informiranje i edukaciju.

Organizacija će poduzeti odgovarajuće Mjere sigurnosti kojima se onemogućuje neovlašten pristup Informacijskom sustavu Organizacije putem interneta, a osobito mjere zaštite od virusa i drugih destruktivnih programa, uključujući instalaciju i pokretanje programa koji služe za zaštitu od virusa na opremi (uređajima) koja se koristi za pristup internetu.

Programi koji služe za zaštitu od virusa moraju biti redovito ažurirani, a Ovlaštene osobe ne smiju isključivati ili onemogućavati takva ažuriranja i programe.

Ovlaštene osobe su dužne izbjegavati internetske aktivnosti koje bi mogle ugroziti sigurnost njihovih računala i Informacijskog sustava Organizacije te prilikom korištenja interneta smiju posjećivati samo stranice koje su neophodne za obavljanje posla.

**5.6. Dodatne mjere zaštite**

U cilju zaštite Informacijskog sustava, Organizacija provodi i sljedeće mjere zaštite:

* Mjere zaštite za sprječavanje neovlaštenih osoba od korištenja Informacijskog sustava:

${psis\_03}

* + ${psis\_03\_item}

${/psis\_03}

* Mjere kojima se osigurava da se podaci sadržani u Informacijskom sustavu ne mogu čitati, kopirati, mijenjati ili ukloniti bez odgovarajućeg ovlaštenja tijekom postupka elektroničkog prijenosa, prijevoza ili pohranjivanja na podatkovne medije, te da postoji mogućnost provjere i identifikacije primatelja na koje se žele prenijeti osobni podaci kroz sustave za obradu podataka:

${psis\_04}

* + ${psis\_04\_item}

${/psis\_04}

* Mjere kojima se osigurava da su podaci sadržani u Informacijskom sustavu zaštićeni od slučajnog uništenja ili gubitka:

${psis\_05}

* + ${psis\_05\_item}

${/psis\_05}

1. Prijava Sigurnosnog incidenta

Ovlaštene osobe i vanjski suradnici kojima su dodijeljena ovlaštenja Ovlaštenih osoba, dužne su, bez odgađanja, obavijestiti upravu Organizacije ili Ovlaštenu osobu koju je odredila uprava Organizacije ako saznaju za bilo kakav Sigurnosni incident i za bilo kakvo kršenje odredbi ovog Pravilnika, odnosno ako uoče bilo kakav nedostatak u radu Informacijskog sustava, a osobito u mjerama sigurnosti Informacijskog sustava.

1. Završne odredbe

Prilikom prestanka ugovora o radu ili ugovornog odnosa s Organizacijom, sve Ovlaštene osobe su dužne vratiti opremu Organizacije, kao i svu ostalu imovinu koja im je dodijeljena na korištenje. Također, sve Ovlaštene osobe su dužne predati svu dokumentaciju te sve podatke u vlasništvu Organizacije. Nije dozvoljeno kopiranje i iznošenje Službenih i Osobnih podataka koji su Ovlaštenim osobama bili povjereni.

Ovaj Pravilnik stupa na snagu osam dana od dana objave.

Ovaj Pravilnik će biti na odgovarajući način obznanjen Ovlaštenim osobama, a period prilagodbe za potpunu primjenu ovih Pravila traje mjesec dana od dana donošenja.