Izvršni odbor Saveza udruga osoba s invaliditetom na svojoj sjednici dana 16.10.2025.godine donosi

Pravilnik o informacijskoj sigurnosti

Članak 1.

Ovim Pravilnikom uređuju se pravila postupanja u Savezu udruga osoba s invaliditetom Karlovačke županije, Karlovac, Banjavčićeva 20 (dalje u tekstu: Savez) glede informacijske sigurnosti.

Glavni ciljevi informacijske sigurnosti su sljedeći:

- očuvanje prihvatljive razine rizika informacijske sigurnosti;
- zaštita podataka od neovlaštene ili nezakonite obrade, gubitka, uništenja ili oštećenja;
- stvaranje povjerenja kod korisnika usluga Saveza i poslovnih partnera u sigurnost podataka koji su dani Savezu.
- osiguranje podrške zahtjevima regulatornih tijela po pitanju sigurnosti podataka;
- prevencija moguće štete zbog gubitka, oštećenja, zloupotrebe ili otuđenja podataka.

KOMPONENTE INFORMACIJSKOG SUSTAVA

Članak 2.

Informacijski sustav Saveza čine;

- Fizičke komponente(računala,memorijski uređaji,,ulazno-izlazne jedinice(tipkovnice,monitori,pisači)
- Softverske komponente(programi i upute koje upravljaju fizičkim komponentama i omogućuju obradu podataka. Tu spadaju operativni sustavi,aplikacijski softveri)
- Mreža koja uključuje infrastrukturu koja povezuje hardverske i softverske komponente na način da omogućuje komunikaciju i razmjenu podataka između njih.
- Podaci koji uključuju sve podatke koji se prikupljaju,obrađuju i pohranjuju u sustav putem baza podataka,datoteka.
- Ljudski faktor uključuje sve osobe koje koriste informacijski sustav
- Organizacija koja označava organizacijske postupke i procedure koja određuje kako se informacijski sustav koristi i kako se njime upravlja unutar organizacije

Članak 3.

Korisnici informacijskog sustava Saveza su zaposlenici i volonteri koji u obavljanju poslova koriste informatičku opremu Saveza.
Korisnici su odgovorni za profesionalno, etičko i zakonito korištenje informacijskih resursa koji su im dani na raspolaganje prvenstveno za korištenje u svrhe poslovnih procesa Saveza.
S obzirom da kapaciteti mrežnih i računalnih resursa Saveza imaju svoja ograničenja, od svih korisnika se očekuje korištenje računalnih resursa učinkovito i racionalno te na način koji neće onemogućiti ili smanjiti efikasnost rada drugih korisnika.

Kontrola pristupa informacijama

Članak 4.

Podaci koji su dio informacijskog sustava čine se zaposlenicima i volonterima dostupnima u skladu s potrebama njihovog radnog mjesta, volonterske pozicije koju obavljaju.

Zaposlenici i ostali korisnici informacijskog sustava će u obavljanju svojih radnih zadataka primjenjivati ;

- „politiku čistog stola“ za papirnatu dokumentaciju (ugovori, pravilnici, upute, dopisi, osobni dosjei korisnika i dr.)

- „praznog zaslona“ za opremu za obradu informacija (računala, tableti, mobiteli, prijenosna računala)

U navedeno spadaju posebno sljedeće mjere:

- sve povjerljivi ili osjetljivi podaci moraju biti uklonjeni sa stola i zaključani u ormar ili u posebnu, za to namijenjenu prostoriju, kada je stol prazan i na kraju radnog dana;
- ormari i prostorije s dokumentima koji sadrže povjerljive ili osjetljive podatke moraju biti zatvoreni i zaključani kada nisu u upotrebi. Ključevi se ne smiju ostavljati u vratima ormara;
- zaporke se ne smiju ostavljati na ljepljivim bilješkama postavljene na ili ispod računala, niti ih smiju biti zapisane na lako vidljivim i pristupačnim mjestima.

Članak 5.

Korisnik informacijskog sustava obvezuje se:

- Izabrati kvalitetnu zaporku, osigurati sigurno korištenje i čuvanje zaporke te ju povremeno mijenjati
- Ukoliko u svom radu proizvodi podatke i dokumente, odgovoran je za vjerodostojnost tih podataka te za njihovo čuvanje kao i za izradu sigurnosnih kopija podataka
- U slučaju oštećenja ili kvara računala i/ili komunikacijskog uređaja prijaviti odgovornoj osobi Saveza u što je moguće kraćem roku
- Omogućiti neometani rad prilikom održavanja računala i/ili komunikacijskih uređaja
- Prilikom uporabe Interneta ne upuštati u aktivnosti koje su zakonom određene kao nelegalne
- Izbjegavati aktivnosti koje bi mogle ugroziti sigurnost njihovih računala i informacijskog sustava Saveza

Korisnicima je zabranjeno:

- Isključivanje ili onemogućavanje rada programa za zaštitu od virusa
- Neovlašteno kopiranje na računalo materijala koje je zaštićeno pravom intelektualnog vlasništva, zaštićenih fotografija, tekstova, filmova, glazbe, programa,...
- Namjerno unošenje malicioznih programa u mrežne sustave i servere (npr; virusi,crvi, trojanski konji,...)

- Odavanje svoje lozinke drugim osobama ili dopuštanje uporabe vlastitog korisničkog računa (user account) drugim osobama, neovisno o tome jesu li te osobe zaposlenici ili volonteri Saveza
- Namjerno uzrokovanje sigurnosnih incidenata, pristupanje podacima koji nisu namijenjeni korisniku ili korisničkom računu za koji korisnik nema dozvolu za uporabu
- Neovlašteno dodavanje/mijenjanje hardverske konfiguracije sustava ili dijela sustava (računala)
- Neovlašteno mijenjanje sigurnosnih postavki računala i komunikacijskih uređaja
- Instaliranje i uporaba softvera na način da se krše prava intelektualnog vlasništva (nelicencirani softveri)
- Korištenje neovlaštenih programa koji ne zahtijevaju instalaciju na računalu

Korištenje interneta

Članak 6.

Internet se smije koristiti isključivo u poslovne i edukacijske svrhe povezane sa poslovnim procesima Saveza i potrebama određenog radnog mjesta.
Sve informacije koje korisnici preuzimaju s interneta moraju biti iz vjerodostojnih izvora.
Savez ne preuzima odgovornost za sadržaje koje korisnik pretražuje,pregledava ili preuzima s interneta a koji bi mogli imati neprimjeren ili uvredljiv sadržaj.

Korištenje elektroničke pošte

Članak 7.

Koristiti službenu elektroničku poštu Saveza kao službeno sredstvo komunikacije, vodeći računa o čuvanju ugleda Saveza prilikom sastavljanja iste te biti svjestan da korištenje elektroničkih poruka ne podrazumijeva privatnost i sigurnost samih poruka

Korisnici su dužni slati elektroničkom poštom ili drugim oblicima elektroničke komunikacije samo istinite i pouzdane informacije

Članak 8.

Korisnici ne smiju:

- Kreirati niti pohranjivati materijale čiji je sadržaj uznemiravajući, nepristojan, klevetnički, na bilo koji način neprihvatljiv ili zakonski nedopušten
- Sudjelovati u aktivnostima čija je namjera uznemiravati ili vrijeđati druge osobe, niti na bilo koji način širiti materijale s uvredljivim sadržajem
- Komunicirati s osobom koja u porukama koristi pseudonim ili zadržava anonimnost
- Otvarati/spremati sadržaj niti odgovarati pošiljatelju u slučaju primitka unaprijed nezatraženog komercijalnog e-maila (sa ili bez priloga).
- Slati ili prenositi sadržaje koji nude usluge ili proizvode u obliku lančanih pisama
- Objavljivati sadržaje na internetu bez suglasnosti vlasnika sadržaja

- Slati poruke koje sadrže podatke ili informacije protivno važećim sigurnosnim pravilima Saveza

Korisnici su dužni:

- Pružiti točne podatke o svom identitetu prilikom slanja poruka elektroničke pošte
- Elektroničkom poštom ili drugim oblicima elektroničke komunikacije slati samo istinite i pouzdane informacije
- Poruke elektroničke pošte koje sadrže poslovne podatke za pojedine poslovne transakcije, za donošenje budućih poslovnih odluka ili korištenje za donesene poslovne odluke, pohraniti sukladno uputama nadređene osobe
- Bez prethodnog odobrenja izvornog pošiljatelja, nije dopušteno takve poruke prosljeđivati u vanjsko okruženje. Od ove odredbe može se odstupiti samo ako se nedvojbeno radi o javnim podacima.

Članak 9.

Korisnici se upozoravaju da nije uputno otvarati privitke elektroničkoj pošti osim kada postoji potvrda slanja od strane pošiljatelja i kada se automatskom provjerom utvrdi odsutnost virusa i drugog zlonamjernog softvera. Prilozi nepoznatih pošiljatelja su primarni izvori računalnih virusa i treba im pristupati s najvišom razinom opreza.

U slučaju dobivanja sumnjive elektroničke pošte postupati s razumnim oprezom te ne slijediti linkove i ne otvarati priloge koji se nalaze u elektroničkoj poruci, ukoliko je vjerodostojnost pošiljatelja upitna. O svim takvim porukama potrebno je odmah obavijestiti odgovornu osobu Saveza

Sve izlazne poruke elektroničke pošte koje se šalju poslovnim partnerima, klijentima, trećim stranama itd., moraju sadržavati slijedeću izjavu o odricanju od odgovornosti na hrvatskom i engleskom jeziku.

IZJAVA O ODRICANJU ODGOVORNOSTI: Ova elektronička poruka i njoj priložene datoteke mogu sadržavati povjerljive i/ili zakonski zaštićene informacije. Ukoliko ste primili ovu poruku, a niste njezin naznačeni primatelj, poruku i sve njezine privitke trajno uklonite, a da ih prethodno ne pročitate ili pohranite na bilo koji način. Svako prenošenje, kopiranje, neovlaštena uporaba ili objavljivanje informacija sadržanih u poruci trećim osobama zabranjeni su i podliježu kaznenoj odgovornosti i građansko - pravnoj zaštiti. Sva odgovornost za viruse i druge štetne programe eventualno sadržane u ovoj poruci isključena je do maksimalne razine dozvoljene zakonom.

DISCLAIMER: This e-mail and its attached files may contain confidential and/or legally protected information. If you received this e-mail and you are not its intended recipient, permanently remove the e-mail and its attached files without reading or saving in any matter. Any disclosure, copying, unauthorized use or publishing of information contained in the e-mail to third parties is prohibited and punishable by civil and criminal liability. All liability for any damage caused by viruses and other malicious program potentially transmitted by this e- mail is excluded to the fullest extend permitted by law.

Korištenje mobilnih uređaja

Članak 10.

Savez dozvoljava svojim zaposlenicima i volonterima korištenje službenih prijenosnih uređaja kao što su mobiteli, dlanovnici, prijenosna računala i sl.
Zaposlenicima i volonterima nije dopušteno;

- posuđivanje mobilnih uređaja drugim osobama u radnom okruženju,članovima obitelji i svim drugim osobama.
- Na mobilne uređaje instalirati nelicencirane ili zlonamjerne aplikacije kao i aplikacije koje nisu nužne za poslovne procese Saveza
- iznošenje podataka, mobilnih uređaja na kojima su isti pohranjeni niti opreme koja je dio informacijskog sustava van službenih prostorija Saveza bez dopuštenja odgovorne osobe Saveza .

Na svim uređajima koji to podržavaju mora se instalirati antivirusna zaštita koja se mora održavati prema naputcima proizvođača.
Za prijenosne uređaje potrebno je koristiti lozinku ili PIN kako bi se onemogućila neovlašteno korištenje uređaja.

Pravila o antivirusnoj i malware zaštiti

Članak 11.

Kako bi se spriječila infekcija informacijskoj sustava Saveza i izbjegle potencijalno teške posljedice takve infekcije, Savez će postaviti odgovarajuće mjere zaštite.

Vatrozid će biti instaliran na svim mjestima na kojima je interna mreža povezana s internetom. Dozvole pristupa moraju biti postavljene tako da korisnik ne može onemogućiti vatrozid.

Članak 12.

Komercijalna i podržana antivirusna platforma će se instalirati na ključnim lokacijama:

- vatrozidu;
- poslužiteljima e-pošte;
- proxy poslužiteljima;
- svim ostalim poslužiteljima;
- svim korisničkim računalima;
- Mobilnim uređajima.

Svi antivirusni programi bit će postavljeni tako da se redovito ažuriraju. U zadanim postavkama protuvirusnih programa, prilikom skeniranja pristupa mora biti omogućeno pružanje zaštite u stvarnom vremenu. Redovita puna skeniranja moraju se provesti jednom tjedno. Korisnici ne smiju onemogućiti antivirusnu zaštitu na uređajima koje koriste.

Članak 13.

U informacijskom sustavu Saveza instalirat će se sustav za filtriranje neželjenih i potencijalno štetnih poruka e-pošte (neželjene pošte). Filtriranje mora osigurati da vrste privitaka koji često sadrže zlonamjerni softver budu blokirane ili uklonjene prije isporuke korisniku.

Članak 14.

Informacije o ranjivosti software-a prikupit će se od dobavljača software-a, odnosno, po potrebi od trećih strana te će se, tamo gdje je to moguće, ažuriranja automatski primjenjivati. Skeniranje ranjivosti mora se redovito provoditi.

Sigurnosni incidenti

Članak 15.

Korisnici informacijskog sustava su dužni nadređenoj osobi prijaviti svaki sigurnosni incident kao i sumnju na potencijalni sigurnosni incident koji ugrožava ili bi mogao ugroziti sigurnost informacijskog sustava Saveza.

Članak 16.

Korisnici su dužni ;

- Izabrati kvalitetnu zaporku, osigurati sigurno korištenje i čuvanje zaporke te ju povremeno mijenjati
- Izbjegavati aktivnosti koje bi mogle ugroziti sigurnost njihovih računala i informacijskog sustava Saveza

U slučaju da korisnici iz vanjskih izvora prime obavijest o pojavi virusa ili neke druge sigurnosne prijetnje o tome su odmah obvezni obavijestiti nadređenu osobu. Nije dopušteno takve obavijesti proslijediti drugim korisnicima u obliku masovne ili lančane elektroničke pošte.

Edukacija o informacijskoj sigurnosti

Članak 17.

Savez će provoditi edukaciju o informacijskoj sigurnosti za sve koji koriste informacijski sustav Saveza. Edukacija je usmjerena podizanju razine informiranosti i svjesnosti u području informacijske sigurnosti u odnosu na moguće rizike u korištenju sustava i funkcije i odgovornosti korisnika sustava.
Svaki novi korisnik sustava mora proći edukaciju koja se odnosi na sigurnosne zahtjeve,ispravnu uporabu informacijske opreme te upoznavanje sa internim propisima o provedbi mjera informacijske sigurnosti.

Članak 18.

Primjena Pravilnika je obvezna za sve zaposlenike,vanjske suradnike,volontere u obavljanju poslova iz djelokruga Saveza. Nepridržavanje zahtjeva iz Pravilnika o informacijskoj sigurnosti od strane zaposlenika smatra se povredom obveza iz ugovora o radu a povreda Pravilnika od strane vanjskih suradnika ili volontera povredom ugovornih obveza i odnosa.

Članak 19.

Zaposlenici i volonteri Saveza kao korisnici informacijskog sustava Saveza po stupanju na snagu Pravilnika informacijske sigurnosti odnosno prije početka korištenja sustava, upoznat će se s Pravilnikom informacijske sigurnosti i najčešćim rizicima.

Članak 20.

Zaštita osobnih podataka uređena je Pravilnikom o zaštiti osobnih podataka.

Članak 21.

Pravilnik o informacijskoj sigurnosti treba se provjeravati i usklađivati s rezultatima provjere sustava upravljanja informacijskom sigurnošću te promjenama u organizacijskom okruženju, poslovnim prilikama, zakonskim propisima i tehnologijama uslijed kojih je potrebna njena prilagodba i poboljšanje. Za provjeru i ažuriranje Pravilnika odgovorna je osoba koju Savez za to zaduži.

Ovaj Pravilnik stupa na snagu i primjenjuje se danom donošenja.