RRiF Učilište za poduzetništvo, (dalje: Voditelj obrade) temeljem Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27.4.2016. godine (dalje: Uredba):
dana 23.05.2018.godine, donosi:

PRAVILNIK O SIGURNOSTI ICT INFRASTRUKTURE

1. UVOD

Članak 1.

Ovaj pravilnik ima za cilj ima definirati sigurnosne zahtjeve koji osiguravaju pravilnu i sigurnu upotrebu informatičke infrastrukture.

Cilj ovog dokumenta je definirati pravila kojima se Voditelj obrade i svi korisnici štite u najvećoj mogućoj mjeri od sigurnosnih prijetnji koje bi mogle ugroziti integritet privatnosti njezinih zaposlenika, suradnika kao i Voditelja obrade.

Ovaj Pravilnik propisanim pravilima osigurava najoptimalniju razinu zaštite osobnih podataka povjerenih na obradu Voditelju obrade, a u skladu sa zahtjevima opće Uredbe o zaštiti osobnih podataka (dalje: Uredba).

Pod pojmom „Informatička infrastruktura“ u ovom Pravilniku podrazumijeva se i hardverska i programska infrastruktura.

Članak 2.

Ovaj Pravilnik odnosi se na sve korisnike informatičke infrastrukture kod Voditelja obrade uključujući i privremene korisnike (gosti, vanjski suradnici) koji imaju privremeni pristup uslugama informatičke infrastrukture te partnere s ograničenim ili neograničenim vremenom pristupa uslugama informatičke infrastrukture.

Ovaj pravilnik zahtjeva i pretpostavlja usklađenost svih korisnika usluga informatičke infrastrukture Voditelja obrade s ovim Pravilnikom.

Članak 3.

Voditelj obrade odgovoran je za sigurnost informatičke infrastrukture, primjenjuje i omogućava prava pristupa podacima i resursima, te djeluje u skladu s Pravilnikom o zaštiti osobnih podataka.

Članak 4.

Svi korisnici upoznati su i prihvatili ovaj Pravilnik, te svi prijavljuju bilo kakav pokušaj povrede sigurnosti informatičke infrastrukture Voditelju obrade odmah po saznanju za povredu.

Članak 5.

Svaki izuzetak od pravila definiranih u bilo kojem dijelu ovog Pravilnika može biti odobren od strane Voditelja obrade.

Svako odstupanje od pravila propisanih ovim Pravilnikom evidentira se zapisnički, evidentirajući vrijeme, opis, razlog odstupanja te način upravljanja rizikom.

Usluge koje omogućuje informatička infrastruktura moraju se koristiti isključivo u skladu s tehničkim i sigurnosnim zahtjevima definiranim ovim Pravilnikom.

2. PRAVILA INFORMATIČKE INFRASTRUKTURE

Članak 6.

Pravila opisana u ovom dijelu odnose se na stolna računala, prijenosna računala, pisače i drugu infrastrukturu, aplikacije i softver te na bilo koga tko upotrebljava tu imovinu, uključujući interne korisnike, privremene zaposlenike, posjetitelje i vanjske suradnike, te sve ostale fizičke i pravne osobe koje rade za i kod Voditelja obrade

Članak 7.

Sva informatička infrastruktura može se koristiti isključivo u poslovnim aktivnostima za koje je namijenjena.

Svaki korisnik je odgovoran za očuvanje i ispravnu upotrebu informatičke infrastrukture koja mu je dana na korištenje.

Sva informatička infrastruktura osim klijentske opreme mora biti na mjestima s ograničenim pristupom.

Pristup infrastrukturi nije dozvoljen neovlaštenim osobama. Dodjeljivanje pristupa informatičkoj infrastrukturi i računalnim mrežama mora se obaviti putem odobrenih i prihvaćenih postupaka za upravljanje uslugama informatičke infrastrukture i nadziranim upravljanjem pristupom.

Članak 8.

Korisnici se moraju prema infrastrukturi, koja im je povjerena na korištenje, odnositi s punom pažnjom, održavati ju čistu te s njom pažljivo rukovati te izbjegavati nepravilno korištenje.

Prijenosna računala tvrtke, tableti, pametni telefoni i ostala infrastruktura koja se koristi na izdvojenim lokacijama mora se periodički održavati i provjeravati svaka 3 mjeseca, a po potrebi i češće, s tim da se svaka provjera mora dokumentirati.

Voditelj obrade jedini je odgovoran za održavanje, nadogradnju i konfiguriranje informatičke infrastrukture. Niti jedan drugi korisnik nije i ne može biti odgovoran i ovlašten za održavanje i nadogradnju infrastrukture, a što uključuje izmjenu hardvera ili instaliranje softvera.

Članak 9.

Posebna se pažnja mora posvetiti zaštiti prijenosnih računala, tableta, pametnih telefona i drugih prijenosnih uređaja od krađe ili gubitka, s tim da se u obzir treba uzeti druge rizike oštećenja infrastrukture te oštećenja koji mogu rezultirati povredom ili gubitkom podataka kao što su ekstremne temperature, magnetska polja ili padovi.

Uvijek kada je moguće, neophodno je koristiti tehnologiju šifriranja i brisanja u slučaju gubitka ili krađe telefona ili tableta.

Članak 10.

Gubitak, krađa, oštećenje, neovlašteno korištenje ili drugi incidenti moraju se odmah prijaviti Voditelju obrade.

Zbrinjavanje informatičke opreme koja se više ne koristi mora se izvršiti u skladu s posebnim postupcima zbrinjavanja informatičkog otpada, uzimajući u obzir zaštitu svih informacija koji su predmet takvog oblika obrade.

Informatička oprema koja pohranjuje povjerljive podatke mora biti uništena, s tim da se sredstva za čuvanje osjetljivih informacija moraju prije odlaganja u potpunosti izbrisati.

3. PRAVILA KONTROLE PRISTUPA

Članak 11.

Pravila kontrole pristupa odnosi se na sve korisnike informatičke infrastrukture kod Voditelja obrade uključujući i privremene korisnike (gosti, posjetitelji, vanjski suradnici) koji imaju privremeni pristup informatičkih uslugama te partnere s ograničenim ili neograničenim vremenom pristupa uslugama koje pruža informatička infrastruktura. Politika zahtjeva i pretpostavlja usklađenost svih korisnika informatičkih usluga Voditelja obrade s propisanom politikom.

Članak 12.

Svaki sustav koji obrađuje podatke mora biti zaštićen sustavnom kontrole pristupa koji se temelji na lozinki.

Minimalno jednom godišnje potrebno je provesti kontrolu i reviziju dodijeljenih prava pristupa.

Svi se moraju suzdržavati od pokušaja manipuliranja ili izbjegavanja kontrole pristupa kako bi dobili veća prava pristupa od onih koja su im dodijeljena.

Članak 13.

Sustav mora uključivati automatsku kontrolu, bilježenje i sprečavanje pokušaja neovlaštenih pristupa kako bi se otkrili svi pokušaji zaobilaženja sustava kontrole i nadzora sigurnosti informatičkog sustava.

4. PRAVILA KONTROLE LOZINKI

Članak 14.

Pravila kontrole pristupa odnosi se na sve korisnike informatičke infrastrukture kod Voditelja obrade uključujući i privremene korisnike (gosti, posjetitelji, vanjski suradnici) koji imaju privremeni pristup informatičkim uslugama te partnere s ograničenim ili neograničenim vremenom pristupa informatičkim uslugama. Politika zahtjeva i pretpostavlja usklađenost svih korisnika informatičkih usluga Voditelja obrade s propisanom politikom.

Članak 15.

Pravila kontrole lozinki su sljedeća:

- Svaki sustav koji obrađuje podatke mora biti zaštićen sustavnom kontrole pristupa koji se temelji na lozinki,
- Svaki korisnik mora imati zasebni privatni identitet za pristup mrežnim uslugama,
- Identiteti moraju biti centralno kreirani i upravljani.
- Svaki identitet mora imati jaku, privatnu alfanumeričku lozinku za pristup uslugama informatičkog sustava,
- Lozinke moraju imati minimalno 7 znakova,
- Lozinke moraju biti sastavljene od kombinacije slova, brojeva i posebnih znakova (interpunkcijskih oznaka i simbola, valute),
- Lozinke moraju imati kombinaciju velikih i malih slova,
- Lozinke ne smiju sadržavati očiti slijed znakova na tipkovnici (npr qwertz ili 12345)
- Lozinke ne smiju sadržavati pogodne podatke kao što su osobni podaci o sebi, članovima obitelji, kućnim ljubimcima, vašoj djeci, rođendanima, adresama, telefonskim brojevima, lokacijama i sl.,
- Dozvoljava se zamjena brojeva za slova npr. „Z“ se može koristiti kao 7, „I“ kao 1 ili „O“ kao 0,

- Pamćenje lozinki ne mora biti teško. Dozvoljeno je korištenje kratkih rečenica kao lozinki (npr. mL@d0$t),
- Svaki redoviti korisnik istu lozinku može koristiti najviše 6 mjeseci , stoga će se lozinka mijenjati svakih 6 mjeseci,
- Ne preporuča se korištenje iste lozinke za pristup različitim sustavima.
- Nitko od zaposlenika Voditelja obrade, nije ovlašten tražiti, prikupljati i pohranjivati lozinke zaposlenika,
- Neprihvatljivo je korištenje administrativne lozinke za neadministrativni rad. Administrator(i) informatičke infrastrukture mora(ju) imati odvojene lozinke za administrativni i neadministrativni rad,
- Strogo je zabranjeno dijeljenje lozinki,
- Lozinke se ne smiju otkrivati ili javno prikazivati,
- Lozinke se ne smiju zapisivati,
- Zabranjeno je slanje lozinki elektroničkom poštom,
- Zabranjeno je spremanje lozinke na računalu,
- Uvijek kada se lozinka smatra kompromitiranom, odmah se mora promijeniti.

5. PRAVILA ELEKTRONIČKE POŠTE

Članak 16.

Pravila elektroničke pošte odnosi se na sve korisnike elektroničke pošte kod Voditelja obrade, neovisno radi li se o privatnim ili služenim adresama elektroničke pošte.

Članak 17.

Pravila elektroničke pošte su sljedeća:

- Sve dodijeljene adrese elektroničke pošte i mjesta za pohranu pošte moraju se koristiti isključivo u poslovne svrhe u interesu Voditelja obrade,
- Povremeno korištenje osobne e-mail adrese na internetu za osobnu namjenu može biti dopušteno ako korištenje ne uzrokuje vidljivu potrošnju resursa Voditelja obrade i ne utječe na produktivnost rada,
- Strogo je zabranjeno korištenje resursa organizacije za neovlašteno oglašavanje, neželjenu elektroničku poštu, političke kampanje i drugo korištenje koje nije povezano s poslovanjem Voditelja obrade,
- Ni na koji način se resursi i adrese elektroničke pošte ne smiju koristiti za otkrivanje povjerljivih ili osjetljivih informacija koje posjeduje Voditelj obrade, osim u slučaju otkrivanja podataka ovlaštenim osobama i na autorizirane adrese elektroničke pošte,
- Korištenje resursa i adresa elektroničke pošte Voditelja obrade za širenje poruka koje se smatraju uvredljivima, rasističkim ili na bilo koji način protivnih zakonu i etici Voditelja obrade apsolutno se zabranjuju,

- Elektronička pošta Voditelja obrade koristi se samo u mjeri koja je potrebna za obavljanje poslovnih zadaća.
- U slučaju da korisnik i Voditelj obrade prekinu poslovni odnos, adresa elektroničke pošte mora biti deaktivirana,
- Korisnici moraju imati privatni identitet da bi pristupili vlastitoj elektroničkoj pošti i resursima za pohranu elektroničke pošte osim u posebnim slučajevima kada pristupaju elektroničkoj pošti dodijeljenoj grupi djelatnika,
- Identiteti za pristup korporativnoj elektroničkoj pošti moraju biti zaštićeni jakim lozinkama. Složenost i trajanje lozinki definirano je ovim Pravilnikom,
- Dijeljenje lozinki nije dozvoljeno. Korisnici ne smiju lažno predstavljati drugog korisnika.
- Antivirusna zaštita i zaštita od zlonamjernih programa mora biti postavljena na svakom klijentskom računalu i na poslužiteljima, kako bi se osigurala maksimalna zaštita od zlonamjerne dolazne i odlazne pošte,
- Sigurnosni incidenti moraju se prijaviti i obraditi što je prije moguće u skladu s procesima upravljanja informacijskom sigurnošću, korisnici ne bi trebali sami odgovarati na sigurnosne napade,
- Sadržaj elektroničke pošte Voditelja obrade treba pohranjivati centralno na mjestima koja se mogu sigurnosno kopirati i s kojima se može upravljati i skladu s procesima Voditelja obrade,

6. PRAVILA KORIŠTENJA INTERNETA

Članak 18.

Pravila korištenja interneta odnosi se na sve korisnike interneta kod Voditelja obrade, uključujući i privremene korisnike (gosti, posjetitelji, vanjski suradnici) koji imaju privremeni pristup internetu tē partnere s ograničenim ili neograničenim vremenom pristupa internetu. Pravila zahtijevaju i pretpostavljaju usklađenost svih korisnika interneta s ovim Pravilnikom.

Članak 19.

Pravila korištenja interneta su sljedeća:

- Za sve korisnike interneta dopušten je ograničen pristup,
- Strogo je zabranjen pristup pornografskim web stranicama i svim drugim rizičnim stranicama.
- Pristup internetu uglavnom je predviđen za poslovnu namjenu. Dopušten je ograničen pristup internetu u osobne svrhe uz uvjet da se vidljivo ne troše resursi Voditelja obrade i ne utječe na produktivnost rada,
- Ulazni i izlazni promet kontroliraju se i ograničavaju pomoću vatrozida,
- Pri pristupanju internetu, korisnici se moraju ponašati u skladu s pravilima koja osiguravaju ugled Voditelja obrade,

- Svaki napad treba biti zabilježen, a ovisno o tipu napada i prijavljen Voditelju obrade odmah po saznanju za napad,
- Potrebno je poduzeti razumne mjere za otkrivanje, sprečavanje i pohranu informacija o napadima na servere i radne stanice.

7. PRAVILA ANTIVIRUSNE ZAŠTITE

Članak 20.

Pravila se odnose na poslužitelje, radne stanice i infrastrukturu kod Voditelja obrade uključujući prijenosna računala koja mogu biti korišteni izvan prostora Voditelja obrade. Neka od navedenih pravila odnose se i na uređaje koji pristupaju resursima Voditelja obrade.

Članak 21.

Pravila antivirusne zaštite su sljedeća:

- Sva računala i uređaji koji pristupaju mreži Voditelja obrade moraju imati instaliranu antivirusnu zaštitu u skladu s najvišim standardima zaštite resursa i informacija,
- Svi poslužitelji i radne stanice u vlasništvu Voditelja obrade ili trajno korišteni uređaji, moraju imati odobreni, centralno upravljani antivirusni program. Ovo pravilo se odnosi i na prijenosna računala koja se redovito povezuju s mrežom Voditelja obrade ili kojima se internetom upravlja putem sigurnih kanala,
- Prijenosna računala koja se rijetko povezuju s mrežom Voditelja obrade, mogu imati instaliran odobreni antivirusni program koji je upravljan lokalno (ne centralno),
- Svi instalirani antivirusni programi moraju se automatski ažurirati te se ažuriranje mora nadgledati kako bi se osiguralo uspješno ažuriranje.

8. PRAVILA KLASIFICIRANJA INFORMACIJA

Članak 22.

Pravila klasificiranja informacija definira okvir za klasificiranje informacija prema važnosti i rizicima koji su uključeni. Cilj je osigurati odgovarajući integritet, povjerljivost i dostupnost podataka Voditelja obrade.

Članak 23.

Pravila opisna u ovom Pravilniku odnose se na sve informacije koje su kreirane, u vlasništvu ili kojima upravlja Voditelj obrade, uključujući one pohranjene u elektroničkom obliku i one tiskane na papiru.

Članak 24.

Pravila klasificiranja informacija su:

- Voditelj obrade mora osigurati sigurnost svih podataka koje posjeduje, neovisno o načinu stjecanja, i osigurati sigurnost sustava koji upravlja podacima u skladu s ovim Pravilnikom i Pravilnikom zaštite osobnih podataka Voditelja obrade,
- Uprava Voditelja obrade odgovorna je za osiguranje i raspodjelu resursa i zadataka koji osiguravaju povjerljivost, cjelovitost i dostupnost informacija, podataka i informatičkih usluga,
- Svaka povreda sigurnosti podataka odmah mora biti prijavljena Voditelju obrade, ravnatelju. Ako je potrebno, moraju se aktivirati odgovarajuće protumjere kako bi se procijenila i kontrolirala eventualno nastala šteta,
- Informacije se razvrstavaju u skladu s njihovim učinkom na sigurnost, s tim da se dijele na 5 kategorija i to: povjerljive, osjetljive, zajedničke, javne i privatne.
- Informacije definirane kao povjerljive imaju najvišu razinu sigurnosti. Samo ograničeni broj osoba može imati pristup tim informacijama. Upravljanje, pristup i odgovornosti vezane uz povjerljive informacije definirane su Pravilnikom o zaštiti osobnih podataka,
- Informacije koje su definirane kao osjetljive mogu biti obrađivane od strane većeg broja osoba. Potrebne su za svakodnevno obavljanje poslova, ali se ne smiju dijeliti izvan dosega potrebnog za obavljanje odgovarajuće funkcije,
- Informacije definirane kao zajedničke, mogu se dijeliti izvan Voditelja obrade, za one klijente, organizacije, korisnike koji imaju pravo im pristupati,
- Informacije definirane kao javne mogu se javno dijeliti, npr. sadržaj na internetskim stranicama,
- Informacije koje se smatraju privatnima pripadaju pojedincima koji su odgovorni za njihovo čuvanje i sigurnosno kopiranje,
- Informacije se klasificiraju zajednički od strane Voditelja obrade i ravnatelja.

9. PRAVILA UDALJENIH PRISTUPA

Članak 25.

Pravila udaljenih pristupa odnosi se na korisnike koji pristupaju unutarnjim resursima Voditelja obrade s udaljenih lokacija.

Članak 26.

Pravila udaljenih pristupa su sljedeća:

- Da bi pristupili internim resursima Voditelja obrade s udaljenih lokacija, korisnici moraju imati potrebna autorizacijska prava. Pristup zaposlenika s udaljenih lokacija može zatražiti samo njemu nadređena osoba, odobrava ga ravnatelj, a omogućava Voditelj obrade.

- Pristup s udaljenih lokacija mora biti omogućen samo sigurnim kanalima uz međusobnu provjeru autentičnosti između poslužitelja i klijenta. I poslužitelj i klijent moraju prepoznati međusobno pouzdane certifikate,
- Nije dozvoljen pristup povjerljivim informacijama s udaljenih lokacija. Iznimka od ovog pravila može se odobriti samo u slučajevima u kojima je to strogo potrebno.
- Korisnici se ne smiju povezivati s javnih računala osim ako se radi o pristupu javnom sadržaju (npr. web stranicama).

Vlasništvo i odobrenje dokumenta

Vlasnik ovog dokumenta je Voditelj obrade i isti mora izvršiti reviziju ovog Pravilnika. Trenutna verzija ovog Pravilnika dostupna je svim zaposlenicima, polaznicima Voditelja obrade i ispitanicima čije osobne podatke Voditelj obrade obrađuje u svojstvu izvršitelja obrade u svom sjedištu.
Pravilnik je odobrio ravnatelj Voditelja obrade dana 23.05.2018.

Odobrio:

dr.sc. Đurđica Jurić

RRiF® 1
UČILIŠTE ZA PODUZETNIŠTVO
ZAGREB — Vlaška 68/I

Evidenciju povijesti promjena, Voditelj obrade vodi u zasebnom dokumentu (koji se vodi pod rednim brojem) koji čini sastavni dio ovog Pravilnika, na način da će svaku promjenu opisati i navesti datum izmijene.

Klasa: 012-04/2018-01/01
Urbroj: 251-396-01-2018-1