

**Sigurnosna politika
informacijskog sustava**

Pravila, preporuke i smjernice za pravilno rukovanje računalnom mrežom i
svim resursima u prostorima škole

**Industrijsko-obrtnička škola Pula
25. svibnja 2018.**

na temelju čl. 3. st. 1. Opće uredbe o zaštiti podataka (EU) 2016/679 i čl. 55. Statuta Industrijsko-obrtničke škole Pula, Školski odbor na sjednici održanoj dana 25. svibnja 2018., donosi

SIGURNOSNU POLITIKU INFORMACIJSKOG SUSTAVA

Uvodne informacije o sigurnosnoj politici

Sigurnosna politika je dokument Industrijsko-obrtničke škole Pula koji definira skup pravila, smjernica i prijedloga o ponašanju prilikom rukovanja informacijskim sustavom u školi i mjerama koje je potrebno poduzeti u konkretnim situacijama. To su mjere koje moraju biti sadržane u organizacijskom i tehničkom dijelu upravljanja informacijskim sustavom koji se koristi za rad srednje škole.

Sigurnosna politika kao dokument je jedan od važnijih dijelova sustava koji definira elemente upravljanje i rada sustavom. Politikom upravljamo sigurnošću informacijskih sustava. Sigurnosna politika je važna za uobičajeno, redovito i kvalitetno funkcioniranje sustava.

Svrha politike sigurnosti je:

1. definirati prihvatljive načine ponašanja,
2. definirati neprihvatljive načine ponašanja,
3. jasno raspodijeliti zadatke,
4. jasno raspodijeliti odgovornosti,
5. propisati smjernice i pravila ponašanja tijekom korištenja informacijskog sustava,
6. propisati sankcije u slučaju nepridržavanja smjernica sigurnosne politike.

Sigurnosna politika Industrijsko-obrtničke škole Pula se odnosi na sve njezine zaposlenike, učenike i osobe koje su tu prisutne po drugim dužnostima, obvezama i razlozima u prostorima škole.

Sigurnosna politika se odnosi na sudionike odgojno obrazovnog procesa i one koji nisu dio tog sustava, a nalaze se u prostorima škole.

Svi zaposlenici, učenici i druge osobe, mogu koristiti informacijski sustav škole pod uvjetima i pravilima koji su propisani za određeni dio informacijskog sustava ili tehničke opreme.

Pravila vrijede za sve jednako i moraju se provoditi na način kako je propisano unutarnjim pravilima škole, zakonima i sigurnosnom politikom.

Pretpostavka sigurnog informacijskog sustava temelji se na ljudima koji se koriste informacijskim sustavom i to isključivo na načine koji su sigurni za cjelokupni sustav.

Tehnologija ne može sama osigurati najvišu razinu sigurnosti, te zbog toga svi moraju imati svoju ulogu te ju savjesno i redovito izvršavati.

Važno je uvesti sve potrebne mjere za očuvanje sigurnosti. Prije svega, to je moguće kroz definiranje sigurnosne politike, krovnog dokumenta za održavanje sigurnosti informacijskog sustava.

Uloga sigurnosne politike je određivanje prihvatljivog i neprihvatljivog načina ponašanja, što joj je i primarna uloga, a cilj je zaštititi vrijednosti informacijskog sustava, opremu, programsku podršku i podatke.

Glavni zadatak sigurnosne politike je osigurati tri jedinstvena svojstva informacija:

- povjerljivost (tajnost);
- integritet;
- dostupnost.

Po definiciji pojmova vrijedi sljedeće:

- povjerljivost se temelji na pretpostavci da se podaci čuvaju u skladu s propisanim zakonima, pravilnicima i drugim propisima u ustanovi;
- integritet se temelji na pretpostavci da su svi podaci cjeloviti i očuvani od vanjskih utjecaja koji mogu integritet narušiti;
- dostupnost se temelji na pretpostavci da su svi podaci dostupni samo onim osobama koje imaju pravo pristupa određenim podacima;

Na temelju čl. 3. st. 1. Opće uredbe o zaštiti podataka (EU) 2016/679 i čl. 55. Statuta Industrijsko-obrtničke škole Pula, Školski odbor na sjednici održanoj dana 25. svibnja 2018., donosi

SIGURNOSNU POLITIKU INFORMACIJSKOG SUSTAVA

Uvodne informacije o sigurnosnoj politici

Sigurnosna politika je dokument Industrijsko-obrtničke škole Pula koji definira skup pravila, smjernica i prijedloga o ponašanju prilikom rukovanja informacijskim sustavom u školi i mjerama koje je potrebno poduzeti u konkretnim situacijama. To su mjere koje moraju biti sadržane u organizacijskom i tehničkom dijelu upravljanja informacijskim sustavom koji se koristi za rad srednje škole.

Sigurnosna politika kao dokument je jedan od važnijih dijelova sustava koji definira elemente upravljanje i rada sustavom. Politikom upravljamo sigurnošću informacijskih sustava. Sigurnosna politika je važna za uobičajeno, redovito i kvalitetno funkcioniranje sustava.

Svrha politike sigurnosti je:

1. definirati prihvatljive načine ponašanja,
2. definirati neprihvatljive načine ponašanja,
3. jasno raspodijeliti zadatke,
4. jasno raspodijeliti odgovornosti,
5. propisati smjernice i pravila ponašanja tijekom korištenja informacijskog sustava,
6. propisati sankcije u slučaju nepridržavanja smjernica sigurnosne politike.

Sigurnosna politika Industrijsko-obrtničke škole Pula se odnosi na sve njezine zaposlenike, učenike i osobe koje su tu prisutne po drugim dužnostima, obvezama i razlozima u prostorima škole.

Sigurnosna politika se odnosi na sudionike odgojno obrazovnog procesa i one koji nisu dio tog sustava, a nalaze se u prostorima škole.

Svi zaposlenici, učenici i druge osobe, mogu koristiti informacijski sustav škole pod uvjetima i pravilima koji su propisani za određeni dio informacijskog sustava ili tehničke opreme.

Pravila vrijede za sve jednako i moraju se provoditi na način kako je propisano unutarnjim pravilima škole, zakonima i sigurnosnom politikom.

Pretpostavka sigurnog informacijskog sustava temelji se na ljudima koji se koriste informacijskim sustavom i to isključivo na načine koji su sigurni za cjelokupni sustav.

Tehnologija ne može sama osigurati najvišu razinu sigurnosti, te zbog toga svi moraju imati svoju ulogu te ju savjesno i redovito izvršavati.

Važno je uvesti sve potrebne mjere za očuvanje sigurnosti. Prije svega, to je moguće kroz definiranje sigurnosne politike, krovnog dokumenta za održavanje sigurnosti informacijskog sustava.

Uloga sigurnosne politike je određivanje prihvatljivog i neprihvatljivog načina ponašanja, što joj je i primarna uloga, a cilj je zaštititi vrijednosti informacijskog sustava, opremu, programsku podršku i podatke.

Glavni zadatak sigurnosne politike je osigurati tri jedinstvena svojstva informacija:

- povjerljivost (tajnost);
- integritet;
- dostupnost.

Po definiciji pojmova vrijedi sljedeće:

- povjerljivost se temelji na pretpostavci da se podaci čuvaju u skladu s propisanim zakonima, pravilnicima i drugim propisima u ustanovi;
- integritet se temelji na pretpostavci da su svi podaci cjeloviti i očuvani od vanjskih utjecaja koji mogu integritet narušiti;
- dostupnost se temelji na pretpostavci da su svi podaci dostupni samo onim osobama koje imaju pravo pristupa određenim podacima;

Svrha politike sigurnosti

1. Prihvatljivo ponašanje

Računalna mreža Industrijsko-obrtničke škole Pula i njezine usluge na raspolaganju su korisnicima radi:

- obavljanja posla,
- učenja, podučavanja, istraživanja,
- usavršavanja u struci,
- drugih razloga koje vodstvo škole daje suglasnost, pismeno ili usmeno

Sva prava korisnici su dužni ostvarivati poštujući potrebe i prava ostalih korisnika informacijskog sustava. Svako korištenje informacijskog sustava je prihvatljivo korištenje, ako se ne krše smjernice i pravila, te ako nisu narušena tuđa prava. Prihvatljiva ponašanja definirana su politikom sigurnosti.

2. Neprihvatljivo ponašanje

Neprihvatljivo ponašanje je svako ponašanje koje nije dopušteno ovim smjernicama ili pravilnikom. Neprihvatljivo je stvaranje ili prijenos datoteka, osim eventualno u okviru znanstvenog istraživanja:

- materijala koji je napravljen da bi izazvao neugodnosti, neprilike ili širio strahove,
- uvredljivog i ponižavajućeg materijala,
- distribuiranje autorski zaštićenih djela bez dozvole vlasnika prava,
- korištenje računalne mreže Industrijsko-obrtničke škole Pulana takav način da ometa korištenje drugim korisnicima,
- širenje, virusa, trojanaca, crva i ostalog zloćudnog softvera,
- slanje neželjenih masovnih poruka,
- preuzimanje tuđeg identiteta,
- provaljivanje na računala koristeći sigurnosne propuste u softveru,
- traženje sigurnosnih propusta na umreženim računalima bez dozvole vlasnika opreme,
- izvršavanje napada uskraćivanjem resursa (Denial of Service),
- korumpiranje ili uništavanje podataka drugih korisnika,
- povreda privatnosti drugih korisnika,
- uništavanje tuđih podataka,
- neovlašteno korištenje tuđih radova,
- kopiranje ili instaliranje softvera za koje ne postoji licenca,
- drugih načina kršenja koji nisu u skladu s općeprihvaćenim normama i standardima.

3. Raspodjela zadataka

Zadaci tijekom nadzora pridržavanja smjernica i pravila sigurnosti u Industrijsko-obrtničkoj školi Pula raspodijeljene su na sljedeći način:

- Odgovorna osoba: preuzima prijave o mogućem kršenju smjernica i pravila ponašanja tijekom korištenja informacijskog sustava, redovito održava dijelove informacijskog sustava, kreira izvješća o obavljenim aktivnostima provedenim na temelju dobivenih prijava;
- Nastavnik informatike: preuzima prijave o mogućem kršenju smjernica i pravila ponašanja tijekom korištenja informacijskog sustava, redovito održava dijelove informacijskog sustava;
- Svi nastavnici: prijavljuju incidente na propisan način, definiraju pravila ponašanja i korištenja računalne opreme, u skladu s propisanim pravilnicima i politikom sigurnosti koja su javno objavljena na webu škole i na oglasnim pločama. Dužni su upozoriti učenike i druge osobe koje se nalaze u školi ukoliko primijete da se radi o ugrožavanju sigurnosti informacijskog sustava;
- Ostali zaposlenici: prijavljuju incidente na propisan način;
- Učenici: prijavljuju incidente na propisan način, sudjeluju u izradi pravila ponašanja za svoje nastavne predmete s predmetnim učiteljem;
- Druge osobe u školi: prijavljuju incidente na propisan način.

Odgovorna osoba, rukovodstvo škole, nastavnici, ostali zaposlenici škole mogu koristiti računalnu opremu za čiju upotrebu imaju dodijeljenu ovlast koristiti je. Učenici mogu koristiti računalnu opremu i mrežu uz dozvolu i prema uputama nastavnika i pod nadzorom nastavnika. Učenici ne smiju bez nadzora nastavnika koristiti mrežnu opremu škole ili računala u učionicama.

4. Raspodjela odgovornosti

Škola ima odgovornu osobu (administrator resursa, administratora e-dnevnika) koji brine o sigurnosti i provođenju smjernica i pravila sigurnosti u školi. Svaka uloga ima definirane svoje ovlasti, prava i obveze koje su u skladu sa zakonom i ostalim propisima. Odgovorna osoba preuzima prijave o incidentima ili eventualnom kršenju pojedinih smjernica ili pravila ponašanja tijekom korištenja informacijskog sustava.

Škola ima nastavnika informatike koji nadzire korištenje sustava na nastavnim satima. On može umjesto odgovorne osobe preuzimati prijave o incidentima ili eventualnom kršenju pojedinih smjernica ili pravila ponašanja tijekom korištenja informacijskog sustava.

Škola ima druge zaposlenike (nastavnike i stručno nenastavno osoblje) koje može koristiti računalnu mrežu. Svi zaposlenici su dužni pridržavati se smjernica i pravila ponašanja tijekom korištenja informacijskog sustava. Sve nepravilnosti su dužni prijavljivati.

Neprijavljivanjem incidenta svaki zaposlenik, učenik ili osoba prisutna u školi koja je to propustila učiniti namjerno, podliježe propisanim sankcijama.

5. Smjernice i pravila ponašanja tijekom korištenja informacijskog sustava

Korištenje informacijskog sustava u kabinetima rukovodstva škole:

- Korištenje informacijskog sustava nije dozvoljeno. Dozvoljeno je samo uz suglasnost ili izričitu dozvolu osobe koja ima pravo pristupa tom dijelu informacijskog sustava.

Korištenje informacijskog sustava u zbornici:

- Korištenje je dopušteno svim zaposlenicima škole u skladu s propisanim smjernicama i pravilima.
- Zauzeće resursa dozvoljeno je u skladu s potrebama.
- Nakon korištenja određenog dijela informacijskog sustava, opremu je potrebno vratiti u stanje u kojemu je zatečena prije korištenja.
- Nakon radnog vremena računalnu opremu je potrebno isključiti na pravilan način. Svi zaposlenici koji koriste računalnu/mrežnu opremu dužni su se educirati, ukoliko ne znaju rukovati spomenutom opremom, kako bi njome mogli na ispravan način rukovati.
- Na računalima nije dozvoljeno korištenje memorija koje nisu očišćene od virusa i drugih malicioznih programa.
- Na računalima se ne smiju pohranjivati osobne datoteke koje nisu potrebne za nastavu i odgojno-obrazovni proces.
- Sve datoteke koje više nisu potrebne se moraju ukloniti. Svaka osoba koja koristi resurse, dužna je nepotrebne datoteke ukloniti.

Korištenje informacijskog sustava u učionicama:

- Korištenje je dopušteno svim zaposlenicima škole u skladu s propisanim smjernicama i pravilima.
- Korištenje je dopušteno učenicima škole samo uz dozvolu nastavnika.
- Učenik resurse koristi samo za one zadatke koje mu je zadao nastavnik.
- Učenik može koristiti računala samo u prisutnosti nastavnika.
- Sve nepravilnosti i kršenja smjernica i pravila, nastavnik prijavljuje na propisan način.
- Zauzeće resursa dozvoljeno je u skladu s potrebama.
- Nakon korištenja određenog dijela informacijskog sustava, opremu je potrebno vratiti u stanje u kojemu je zatečena prije korištenja.
- Nakon radnog vremena računalnu opremu je potrebno isključiti.
- Na računalima nije dozvoljeno korištenje memorija koje nisu očišćene od virusa i drugih malicioznih programa.
- Na računalima se ne smiju pohranjivati osobne datoteke koje nisu potrebne za nastavu i odgojno-obrazovni proces.
- Sve datoteke koje više nisu potrebne se moraju ukloniti. Svaka osoba koja koristi resurse, dužna je nepotrebne datoteke ukloniti.

Računala u informatičkoj učionici, učionici vježbeničkih tvrtki i učionicama u kojima se izvodi nastava na više od jednog računala, vodi se evidencija korištenja računalnih i mrežnih resursa.

Evidencija korištenja resursa podrazumijeva:

- Vlastoručno potpisivanje učenika na potpisnu listu uz oznaku radnog mjesta koje koriste,
- Pregled zatečenog stanja na početku nastavnog sata i prijava svih nedostataka,

- Potpis nastavnika koji je taj sat u učionici održao nastavu,
- Pregled zatečenog stanja od strane nastavnika i potvrda zatečenog stanja.

Evidencija korištenja računalnih/mrežnih resursa omogućuje praćenje stanja u učionicama i lakše pronalaženje osoba koje su uzrokovale kvar u određenom dijelu informacijskog sustava.

Čuvanje osobnih korisnički podataka:

- Korisnički podaci su tajni.
- Svatko je vlasnik svojih korisničkih podataka i dužan ih je čuvati.
- Zabranjeno je ustupanje osobnih korisničkih podataka bilo kojoj drugoj osobi bez obzira na razlog.
- Svaki zaposlenik ima svoju mail adresu oblika **ime.prezime@skole.hr** koju je dobio na korištenje tijekom vremena zaposlenja. To je službena mail adresa škole i svi zaposlenici su dužni provjeravati svoju elektroničku poštu.
- Gubitak podataka se mora prijaviti administratoru škole koji će izdati nove podatke.
- Svi mail računi i drugi računi koji nisu službeni dio komunikacije, ne moraju se prihvaćati od strane drugih zaposlenika sustava kao sredstvo komunikacije.

Zabranjeno je korištenje tuđeg korisničkog računa.

6. Sankcije u slučaju nepridržavanja smjernica sigurnosne politike

Osoba koja namjerno uzrokuje kvar računalne mreže, računala ili bilo kojeg dijela informacijskog sustava, snosi troškove popravka istoga. Drugačije je moguće postupati u slučaju kada je to tako dokazano i moguće. Sva postupanja se moraju voditi u skladu s važećim zakonima, pravilnicima škole i ostalim propisima.

Korištenje e-dnevnika

Industrijsko-obrtnička škola Pula koristi e-Dnevnik od školske godine 2015./2016.

E-Dnevnik je jedan od alata nastavnog osoblja koji su oni dužni poznavati i redovito se educirati o način rada s e-Dnevnikom.

Škola ima administratora e-Dnevnika. Administrator e-Dnevnika izvršava svoje obveze koje su propisane zakonom i važećim pravilnicima. Administrator e-Dnevnika može reagirati samo u slučaju kada zaprimi valjani zahtjev od strane nastavnika. Svaki nastavnik mora na propisani način prijaviti svoj zahtjev i to korištenjem službenog sredstva komunikacije opisanog točkom 5.

Sve upute za nastavnike, moguću edukaciju o korištenju e-Dnevnika i ostale potrebne informacije, nastavnici će dobiti na oglasnoj ploči i službenim mailom koji su dužni redovito provjeravati.

PRILOZI

Prilozi su CARNet-ovi dokumenti koji su izrađeni kao smjernica sigurnosne politike za škole.

Pravilnici CARNet-a su preuzeti uz minimalne prilagodbe.

Pravilnik o rukovanju zaporkama

Pravilnik o korištenju elektroničke pošte

Pravilnik o antivirusnoj zaštiti

Pravilnik o zaštiti od spama

Pravilnik o rješavanju sigurnosnih incidenata

Pravilnik o rukovanju povjerljivim informacijama

Izvori:

http://www.cert.hr/carnet_sigurnosna_politika

http://www.cert.hr/sites/default/files/sigurnosna_politika_ustanove.pdf

Prilozi – dokumenti za samovrednovanje: *

Samovrednovanje – Stvaranje sigurne lozinke

Samovrednovanje – Čuvanje lozinke

Samovrednovanje – Sigurnosna provjera lozinke

Samovrednovanje – Čuvanje podataka elektroničke pošte

Samovrednovanje – Čuvanje medija za pohranu podataka

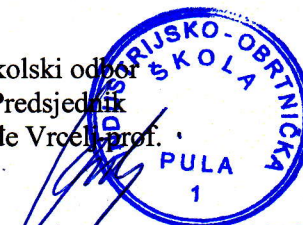
Samovrednovanje – Korištenje antivirusne zaštite

Samovrednovanje – Rješavanje sigurnosnih incidenata

*dokumenti su objavljeni javno i dostupni na računalu u školi

Ova Sigurnosna politika informacijskog sustava stupa na snagu danom objave na oglasnoj ploči Škole.

Školski odbor
Predsjednik
Đorđe Vrceli, prof.



Sigurnosna politika informacijskog sustava je objavljena na oglasnoj ploči Škole dana 25. svibnja 2018., te stupa na snagu 25. svibnja 2018. godine.

Ravnatelj
Petar Gavrić, dipl. ing.



KLASA: 003-05/18-01/02

URBROJ: 2168-22-18-1

Pula, 25. svibnja 2018.