Srednja škola Zvane Črnje Rovinj
Scuola media superior "Zvane Črnja" Rovigno

Sigurnosna politika informacijskog sustava

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

Svibanj, 2020.

Na temelju čl. 3. st. 1. Opće uredbe o zaštiti podataka (EU) 2016/679 i čl. 57. Statuta Srednje škole Zvane Črnje Rovinj – Scuola media superior "Zvane Črnja" Rovigno Školski odbor na sjednici održanoj dana 17. lipnja 2020. donosi

SIGURNOSNU POLITIKU INFORMACIJSKOG SUSTAVA

Sigurnosna politika je dokument Srednje škole Zvane Črnje Rovinj – Scuola media superior "Zvane Črnja" Rovigno (u daljnjem tekstu: Škola) 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 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.

Odnosi se na sudionike odgojna obrazovnog procesa i ostalih koji se nalaze 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 te sukladno sigurnosnoj politici.

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 primama 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 propisima,
- 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 je:

- definirati prihvatljive načine ponašanja,
- definirati neprihvatljive načine ponašanja,
- jasno raspodijeliti zadatke,
- jasno raspodijeliti odgovornosti,
- propisati smjernice i pravila ponašanja tijekom korištenja informacijskog sustava,
- propisati sankcije u slučaju nepridržavanja smjernica sigurnosne politike.

Prihvatljivo ponašanje

Računalna mreža Škole 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.

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 Škole 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.

Raspodjela zadataka

Zadaci tijekom nadzora pridržavanja smjernica i pravila sigurnosti u Školi raspodijeljene su na sljedeći način:

1. 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;
2. Nastavnik informatike: preuzima prijave o mogućem kršenju smjernica i pravila ponašanja tijekom korištenja informacijskog sustava, redovito održava dijelove informacijskog sustava;
3. Svi nastavnici: prijavljuju incident 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;
4. Ostali zaposlenici: prijavljuju incident na propisan način;
5. Učenici: prijavljuju incidente na propisan način, sudjeluju u izradi pravila ponašanja za svoje nastavne predmete s predmetnim učiteljem;
6. Druge osobe u školi: prijavljuju incident odgovornoj osobi;

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.

Raspodjela odgovornosti

Škola ima odgovornu osobu (administrator resursa) koji brine o sigurnosti i provođenju smjernica i pravila sigurnosti u školi. Svaka uloga ima definirate 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 (ostale 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.

Smjernice i pravila ponašanja tijekom korištenja informacijskog sustava

Korištenje informacijskog sustava u uredima 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 radnoj prostoriji:

- 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 potrebni 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, prijavljuju incident odgovornoj osobi.
- 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 potrebni se moraju ukloniti. Svaka osoba koja koristi resurse, dužna je nepotrebne datoteke ukloniti .

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

Evidencija aktivnosti obrade kod online nastave

Tijekom provođenja online nastave provodi se provjera znanja na način koji odgovara pojedinom predmetu, konkretnoj nastavnoj jedinici i ostalim faktorima koji mogu utjecati na sam postupak kako bi bio primjeren svrsi.

Sredstvo provjere može, uz ostalo, biti: usmeni razgovor, komunikacija u živo u razredu ili putem video linka, pisanje na papir u razredu ili dostava elektroničkog dokumenta, naknadna analiza i procjena dostavljenog uratka te audio ili video snimka.

U slučaju kada nastavnik procijeni da je prikladno provesti provjeru znanja korištenjem audio ili video snimke, ista se može snimiti tijekom razgovora ili ju učenik može dostaviti elektroničkom poštom ili drugim prikladnim načinom.

S aspekta zaštite osobnih podataka (GDPR) takvo prikupljanje i obrada osobnih podataka svoju zakonitost ima u Članku 6.1.f (iz razloga nužnosti izvršavanja zadaće od javnog interesa ili pri izvršavanju službene ovlasti) posebno u kurikulu škole.

Ključno je da nastavnik osigura odgovarajuće tehničke i organizacijske mjere zaštite tako prikupljenih podataka (informacijska sigurnost audio i video snimke i meta podataka) i da se obrada provodi isključivo u prvobitnu svrhu (provjera znanja).

Prvo nastavnik treba snimku pohraniti na sigurno mjesto i uništiti sa svih drugih mjesta koja su možda bila korištena u postupku prikupljanja snimke (primjerice pohrana na računalo a brisanje s mobitela ili tableta na kojemu je snimka zaprimljena).

U situaciji rada kod kuće potrebno je osigurati da do snimke ne mogu doći druge osobe kako ne bi došlo do neovlaštenog uvida u podatke (gledanje se smatra obradom podataka!), prosljeđivanje ili njihove objave na društvenim mrežama.

Odmah nakon završetka postupka provjere znanja snimku treba pohraniti na USB stik koji je enkriptiran i snimku izbrisati s računala. Na tom stiku se mogu prikupljati sve snimke koje se više ne obrađuju. U slučaju potrebe poput žalbe učenika moguće je ponovno pregledati pojedinu snimku.

Nakon završetka nastave kada nastavnik pohranjuje u arhivu cjelokupnu dokumentaciju učenika treba također pohraniti i USB stik pri čemu tajništvu dostavlja ključ i broj USB stika.

Period čuvanja je isti kao i kod ostale dokumentacije koja čini arhivu učenika ili razreda.

Brisanje odnosno uništavanje podataka vrši se istekom perioda čuvanja ili stvarnim brisanjem i uništavanjem ili prosljeđivanjem u državni arhiv slijedom procedure koja vrijedi i za pismene radove.

Učenici i roditelji trebaju biti upoznati s mogućnošću provođenja provjere znanja putem audio i video snimke putem " Informacije učenicima i roditeljima o obradi osobnih podataka prilikom korištenja alata za online nastavu u provjeri znanja".

Roditeljima se ta informacija dostavlja na prvom roditeljskom sastanku, učenicima na satu

predmetnog nastavnika. Kada nastavnik odluči bilježiti audio ili video razgovor s učenikom treba prije početka snimanja o obavijestiti učenika. U slučaju kada učenik odbije ili se usprotivi takvom načinu provjere znanja treba proslijediti nadležnim stručnim službama na daljnje odlučivanje.

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.

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 propisima i općim aktima škole.

Korištenje e-Dnevnika

E-Dnevnik je jedan od alata nastavnog osoblja koji su dužni poznavati i redovito se educirati o načinu 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 propisan način prijaviti svoj zahtjev i to korištenjem službenog sredstva komunikacije.

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

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

Predsjednik Školskog odbora
Željko Balog, prof.

Sigurnosna politika informacijskog sustava je objavljena na oglasnoj ploči Škole dana, 18. lipnja 2020. te stupa na snagu dana 18. lipnja 2020.

Ravnateljica:
Ingrid Sau, prof.mentor

SREDNJA ŠKOLA ZVANE ČRNJE ROVINJ ROVIGNO SCUOLA MEDIA SUPERIORE ZVANE ČRNJA

KLASA: 003-05/20-01/02
URBROJ: 2171-08-09-20-01
Rovinj, 18. lipnja 2020.