# OŠ Ferdinandovac - Računalna sigurnost

Sigurnosna politika dio je sustava upravljanja sigurnošću informacijskih sustava. Njezina je svrha da definira prihvatljive i neprihvatljive načine ponašanja, da jasno raspodijeli zadatke i odgovornosti, te da propiše sankcije u slučaju nepridržavanja.

**Na koga se odnosi sigurnosna politika?**

Pravila rada i ponašanja koja definira sigurnosna politika vrijede za:

- Svu računalnu opremu koja se nalazi u prostorima Ustanove.
- Administratore informacijskih sustava
- Korisnike, među koje spadaju: zaposlenici, vanjski suradnici, učenici
- Vanjske tvrtke koje po ugovoru rade na održavanju opreme ili softvera

**Sigurnost školske računalne mreže**

Ciljevi mjera informacijske sigurnosti koje se primjenjuju na školsku računalnu mrežu su, kako slijedi:

1. omogućavanje elektroničke komunikacije,
2. neometano korištenje informacija koje su putem računalne mreže dostupne,
3. zaštita školske računalne mreže,
4. zaštita osjetljivih podataka Škole

Radi lakšeg održavanja potrebno je dokumentirati izgled mreže. Dokumentacija može obuhvaćati grafički prikaz fizičkog rasporeda računala u Školi uključujući osnovne postavke (IP adresa računala), ili popis računala s informacijom gdje su smještena te koje IP adrese imaju dodijeljene.
Bežičnu mrežu (WiFi) potrebno je podesiti tako da samo legitimni korisnici mogu pristupiti i koristiti mrežu. Legitimni korisnici mogu biti nastavno i administrativno osoblje te učenici. Nitko od navedenih korisnika ne smije ometati i onemogućavati rad školske bežične mreže.

Škola zadržava pravo nadzora, filtriranja i korištenja svog mrežnog prometa.

**Sigurnost školskih računala**

Ispravna konfiguracija računala olakšava njihovo održavanje, a ujedno i povećava sigurnost učenika i učitelja odnosno nastavnika. Zato je potrebno da sva računala u školi imaju minimalni skup preporučenih sigurnosnih postavki. Sva računala trebaju imati instaliran antivirusni alat. Neki besplatni antivirusni alati su AVG, Avira, Avast i Security Essentials. Sva računala moraju imati uključen vatrozid (eng. firewall) kako bi se onemogućio pristup do njih s Interneta. Potrebno je redovito ažurirati sve programe na računalima. Korisnici moraju sami pratiti rad antivirusnih alata i o mogućim napadima obavještavati administratore.

Računala moraju biti podešena tako da traže prijavu korisnika (npr. autentikacijom putem AAI sustava) prije početka rada. Preporučuje se korištenje lozinki koje se sastoje od kombinacije malih i velikih slova, brojeva i posebnih znakova te su minimalne duljine 8 znakova.

Učenici na računala ne smiju instalirati nikakve korisničke programe bez dozvole. Ako učenici žele instalirati neke korisničke programe, mogu se obratiti svom učitelju, nastavniku informatike ili ravnatelju škole.

**Sigurnost korisnika**

Podizanje razine svijesti korisnika o važnosti sigurnosti ključno je za uspješno provođenje ovih pravila. Korisnici moraju biti dobro upoznati sa sigurnosnim aspektima pri korištenju računala i mjerama koje proizlaze iz njega, a to se postiže redovitom edukacijom. Potrebno je što više napora uložiti u edukaciju učenika te učitelja i nastavnika o sigurnosnim aspektima prilikom korištenja računala i mobilnih uređaja.

Svi korisnici školskih računala moraju se prijaviti na sustav prije korištenja i odjaviti nakon završetka korištenja. Prijava i odjava korisnika mora uključivati minimalno korištenje korisničkog imena i pripadajuće lozinke.

Ako je nužno proslijediti tuđu elektroničku poruku (eng. e-mail), poruku je potrebno proslijediti bez mijenjanja konteksta i značenja. Prilikom prosljeđivanja tuđe elektroničke poruke potrebno je paziti da se tuđi osobni podaci ne prosljeđuju bez pristanka vlasnika.

Datoteke preuzete iz nekog vanjskog izvora (putem elektroničke pošte, vanjskog diska, ili s Interneta) mogu ugroziti sigurnost učenika ili učitelja odnosno nastavnika. Zato je uputno ne otvarati ili prosljeđivati zaražene datoteke i programe kao niti otvarati datoteke iz sumnjivih

ili nepoznatih izvora. Sve takve datoteke potrebno je provjeriti antivirusnim alatom prije korištenja.

Pravila pristupa učenika i zaposlenika škole školskim računalima potrebno je redovito provjeravati i po potrebi mijenjati. Minimalno jednom godišnje (početkom školske godine) potrebno je revidirati elektroničke identitete (AAI) učenika. Zadnji nastavni dan učenika odnosno radni dan učitelja ili nastavnika u školi potrebno je isključiti sva njegova prava pristupa školskim računalima. Nakon isteka učeničkog statusa i prestanka potrebe za posjedovanjem elektroničkog identiteta učenika, identitet je potrebno isključiti.

Učenici i učitelji smiju koristiti samo školska računala namijenjena njima. Vlastita računala i pametne telefone tijekom nastave učenici smiju koristiti isključivo u obrazovne svrhe uz prethodnu dozvolu učitelja. Pri tome učenici moraju paziti da ne ugrožavaju druge korisnike Školske mreže širenjem virusa i drugih zlonamjernih programa.

Administratori sustava smiju koristiti sva računalna sredstva u otkrivanju nedozvoljenih postupaka na mreži.

Učenici smiju koristiti školska računala u privatne svrhe isključivo u slobodno vrijeme (za vrijeme odmora, te prije ili nakon nastave). Učenici ne smiju ometati druge učenike ili učitelje (ili nastavnike) prilikom korištenja računala tijekom boravka u školi ili oko škole.

Politika prihvatljivog korištenja

Učenike i učitelje se potiče na korištenje informacijskih tehnologija i alata u svrhu unapređenja obrazovanja. Korištenje multimedijskih sadržaja, programa za suradnju i komunikaciju, društvenih mreža te sličnih načina komunikacije tijekom nastave je dozvoljeno samo ako to učitelj ili nastavnik dopusti.

Korisnici školskih računala se moraju ponašati odgovorno i u skladu s etičkim načelima i u stvarnom i u virtualnom svijetu. Prema drugim korisnicima moraju se ponašati pristojno, ne vrijeđati ih niti objavljivati neprimjerene sadržaje.

Prilikom korištenja i objavljivanja sadržaja na Internetu, uputno je da se korisnici pridržavaju sljedećih naputaka:

- *odgovornost za sadržaje* - svi korisnici, a posebice učenici, moraju znati da su odgovorni za sve što pišu, objavljuju ili komentiraju na Internetu. Uvijek moraju imati na umu da i njihova privatna aktivnost u društvenim medijima može utjecati na školske rezultate. Učenici mogu gledati sve učiteljske aktivnosti na Internetu, ali i obrnuto. Svaki korisnik je odgovoran i za sve neželjene posljedice korištenja Interneta. Kako bi se izbjegle neugodne/neželjene situacije predlažemo korisnicima da u svakoj situaciji, gdje god bili i o kojoj god temi objavljivali sadržaje, dobro razmisle o sadržaju koji objavljuju.

- *potpisivanje* - odgovorni korisnici svojim potpisom stoje iza sadržaja koje objave na Internetu. Korisnike se potiče da se, gdje god smatraju primjerenim, predstave svojim imenom. Time nastaje bolja društvena mreža kontakata, a i drugi korisnici će radije koristiti sadržaje iz poznatih izvora.

- *znanje o publici* - uputno je da svatko tko objavljuje sadržaje kroz društvene mreže i medije vodi brigu o publici koja će to čitati. Mogući posjetitelji mogu biti školski kolege, potencijalni poslodavci, suradnici itd.

- *razumijevanje koncepta zajednice* - društvene mreže (zajednice) postoje kako bi se njihovi članovi mogli međusobno podržavati. Zato svaki korisnik mora dobro balansirati između privatnih i školskih informacija koje dijeli s drugima. Vrlo važnu ulogu u razvoju i osnaživanju zajednice imaju otvorenost i transparentnost. Takva zajednica ne potiče suparništvo, već suradnju i međusobno pomaganje.

- *poštivanje autorskih prava* - korisnike se potiče da potpisuju materijale koje su sami izradili, ali i da poštuju tuđe radove. Nipošto ne smiju tuđe radove predstavljati kao svoje, preuzimati zasluge za tuđe radove, niti nedozvoljeno preuzimati tuđe radove s Interneta. Korištenje tuđih materijala s Interneta mora biti citirano, obavezno navodeći autora korištenih materijala.

- *čuvanje vlastite i tuđe privatnosti* - korisnici moraju biti pažljivi koje svoje osobne podatke objavljuju na Internetu jer time utječu na svoju sigurnost i zaštitu svoje privatnosti. Nadalje, korisnici moraju biti svjesni činjenice da kad se jednom podatak pojavi na Internetu više ga nije moguće jednostavno ukloniti.

- *umjerenost u korištenju* - vrlo je bitno dobro uravnotežiti vrijeme odvojeno za korištenje Interneta, s drugim oblicima nastave, učenja i odmora.

Korisnici moraju imati na umu da sadržaji koji se nalaze na Internetu ne moraju biti provjereni niti istiniti. Zato sve činjenice koje nađu na Internetu moraju koristiti s oprezom. Učenici svakako trebaju koristiti informacije s Interneta u skladu s učiteljevim ili nastavnikovim uputama. Svi sadržaji koji se koriste kao izvor informacija za nastavu moraju se koristiti iz provjerenih izvora.

Od učenika se očekuje da prihvate filtriranje određenih sadržaja kao sigurnosnu mjeru, te ga ne smiju pokušati zaobići jer je ono postavljeno radi njihove sigurnosti, ali i sigurnosti svih drugih učenika. Nadalje, zaobilaženje sigurnosnih postavki moglo bi ugroziti održavanje nastave. Ako učenik smatra da je određeni sadržaj neopravdano blokiran ili propušten može se obratiti svom učitelju ili nastavniku ili učitelju informatike. Ako učenici primijete neprimjerene, uznemirujuće ili sadržaje koji ugrožavaju njihovu sigurnost, o tome odmah trebaju obavijestiti svog učitelja odnosno profesora, učitelja informatike ili ravnatelja.

Učenici se moraju pridržavati i drugih uputa koje im mogu dati učitelji ili nastavnici, a koje imaju za cilj unaprjeđenje sigurnosti školske informatičke opreme i mreže.

## RUKOVANJE ZAPORKAMA

1. Minimalna dužina zaporke

Kratku zaporku lakše je probiti. Stoga neka minimalna dužina zaporke bude šest znakova, ali preporučujemo korištenje još dužih zaporki.

2. Ne koristiti riječi iz rječnika

Hackeri posjeduju zbirke rječnika, što im olakšava probijanje ovakvih zaporki (tzv. dictionary attack).

3. Izmiješati mala i velika slova s brojevima

Na primjer: h0bo3niCa. Na prvi pogled besmislena i teška za pamćenje, ova je zaporka izvedena iz riječi hobotnica. Polazište je pojam koji lako pamtimo, ali onda po nekom algoritmu vršimo zamjenu znakova.

4. Ne koristiti imena bliskih osoba, ljubimaca, datume

Takve se zaporke lako otkriju socijalnim inženjeringom.

Tajnost zaporke

5. Korisnici su odgovorni za svoju zaporku i ni u kom je slučaju ne smiju otkriti

Korisnici koji se ne pridržavaju navedenih pravila ugrožavaju sigurnost informacijskog sustava. Ustanova je obavezna odgojno djelovati i obrazovati korisnike u kreiranju sigurnih zaporki.

## ELEKTRONIČKA POŠTA

Elektronička pošta dio je svakodnevne komunikacije, poslovne i privatne. Komuniciranje e-mailom na Ustanovi zahtijeva da se razmotre svi aspekti elektroničke komunikacije s obzirom na moguće posljedice.

Protokol koji se koristi za prijenos elektroničke pošte, SMTP ili Simple Mail Transport Protocol, nije od samog početka dizajniran da bude siguran. Dodatne probleme ponekad izazivaju i korisnici, koji nisu posve svjesni zamki pri korištenju e-maila.

Stoga ćemo se na početku ukratko pozabaviti problemima koji mogu nastati pri korištenju elektroničke pošte.

1. Nesigurnost protokola

• Poruke putuju kao običan tekst, otvorene kao na razglednici, te ih je lako presresti i pročitati, ili čak izmijeniti sadržaj.

• Lako je krivotvoriti adresu pošiljatelja, tako da nikada niste sigurni tko vam je zapravo poslao poruku.

• Protokoli za čitanje elektroničke pošte, POP i IMAP, u svom osnovnom obliku šalju korisničko ime i zaporku kao običan tekst, pa ih je moguće presresti i pročitati. Stoga je potrebno, kad god je to moguće, koristiti kriptografiju, na primjer SSL za prijenos i PGP za skrivanje sadržaja.

2. Nezgode

• Uvijek je moguće pritisnuti pogrešnu tipku ili kliknuti mišem na susjednu ikonu. Time može nastati nepopravljiva šteta – ne možete zaustaviti poruku koja je već otišla. Ako se umjesto Reply pritisne Reply All, poruka će umjesto jednom primatelju otići na više adresa, a povjerljive informacije dospjeti do neželjenih primatelja.

• Česta je pogreška i kada se pokupi pogrešna adresa iz adresara.

• Neki mail klijenti sami dovršavaju e-mail adresu koju tipkate. U žurbi se može prihvatiti pogrešna adresa, slična onoj koju zapravo želite.

3. Nesporazumi

• Ljudi su skloni pisati e-mail poruke na ležerniji, opušteniji način. To može dovesti do nesporazuma ako druga strana ne shvaća poruku na isti način. Stoga službene dopise pišite u službenom tonu.

• Iza vašeg imena u e-mail adresi nalazi se ime ustanove. Pišući, budite svjesni da netko može shvatiti vašu privatnu prepisku kao službeni dopis, vaše privatno mišljenje kao službeni stav ustanove. Stoga u raspravi uvijek jasno naznačite kada

je izneseni stav vaše privatno uvjerenje.

Pravilnik o korištenju elektroničke pošte (prijedlog), prosinac, 2003. 17/29CARNet

4. Otkrivanje informacija

• Poruke namijenjene jednoj osobi, začas se mogu proslijediti drugima, na primjer na mailing listu. To se može dogoditi

o (zlo)namjerno, s ciljem da se naškodi drugoj osobi ili tvrtki

o nemarom sudionika, koji ne traži dozvolu za prosljeđivanje poruke

o slučajnom omaškom, na primjer nehotičnim klikom mišem na pogrešnu ikonu (Reply All umjesto Reply)

• Stoga poslovne dopise koji sadrže osjetljive informacije treba označiti kao povjerljive, kako bismo primatelja obavezali na diskreciju.

• U slučaju sigurnosnog incidenta, istraga može dovesti do otkrivanja sadržaja poruka koje su zamišljene kao privatna komunikacija. Ustanova se obavezuje čuvati povjerljivost takvih poruka, ali to ne može garantirati ako poruke budu tretirane kao dokazni materijal u istrazi ili u mogućem sudskom procesu.

5. Radna etika

• Velika količina poruka koje treba svakodnevno pročitati može vam oduzeti znatan dio radnog vremena. Stoga ograničite broj privatnih i zabavnih poruka.

• Lančane poruke koje ljudi šalju poznanicima mogu sadržavati lažne informacije ili biti dio prijevare, s namjerom da se ljudima izvuče novac ("pomozite nesretniku kojem treba operacija", "otvorite račun kako bi svrgnuti diktator mogao izvući novac iz nestabilne afričke države"...). Za provjeru ovakvih poruka (engl. hoax) može se koristiti servis CARNet CERT-a "Hoax recognizer"

• Spam, slanje neželjenih komercijalnih poruka, sve više opterećuje promet na Internetu, te oduzima vrijeme, čak i ako brišete takve poruka bez čitanja. Ustanova će filtrirati spam na poslužitelju elektroničke pošte, ali je obaveza korisnika da sami

ne šalju takve poruke.

6. Povreda autorskih prava

• Svaka poruka elektroničke pošte može se smatrati autorskim djelom, stoga ona pripada osobi koja ju je poslala. Stoga za prosljeđivanje tuđe poruke morate tražiti dozvolu njezina autora.

• Prilozi koji se šalju uz elektroničke poruke mogu sadržavati autorski zaštićene informacije, na primjer glazbu, filmove, članke itd. Primajući i šaljući takve sadržaje možete izložiti tužbi ne samo sebe, već i Ustanovu.

Zbog svega nabrojanog korištenje elektroničke pošte smatra se rizičnom djelatnošću, te se korisnici obavezuju na pridržavanje određenih pravila:

• Zaposlenicima se otvara korisnički račun radi obavljanja posla.

• Privatne poruke dozvoljene su u umjerenoj količini, ukoliko to ne ometa rad. Za privatne potrebe mogu se koristiti za to namijenjene HR-F domene.

• Pišući poruke, budite svjesni da ne predstavljate samo sebe, već i ustanovu za koju radite.

Pravilnik o korištenju elektroničke pošte (prijedlog), prosinac, 2003. 18/29 CARNet

• Pridržavajte se netikete, pravila pristojnog ponašanja na Internetu, službenu e-mail adresu nemojte koristiti za slanje uvredljivih, omalovažavajućih poruka, ili za seksualno uznemiravanje.

• Nije dozvoljeno slanje lančanih poruka kojima se opterećuju mrežni resursi i ljudima oduzima radno vrijeme.

• Svaka napisana poruka smatra se dokumentom, te na taj način podliježe propisima o autorskom pravu i intelektualnom vlasništvu. Nemate pravo poruke koju su poslane vama osobno proslijediti dalje bez dozvole autora, odnosno pošiljatelja.

• Sve poruke pregledati će automatski aplikacija koja otkriva viruse. Ako poruka zadrži virus, neće biti isporučena, a pošiljatelj i primatelj će biti o tome obaviješteni. Poruka

će provesti određeno vrijeme u karanteni, odakle ju je moguće na zahtjev primatelja izvući. Nakon određenog vremena, obično mjesec dana, poruka se briše iz karantene kako bi se oslobodio prostor na disku.

• Ustanova zadržava pravo filtriranja poruka s namjerom da se zaustavi spam.

• U slučaju istrage uzrokovane mogućim sigurnosnim incidentom, sigurnosni tim može pregledavati kompletan sadržaj diska, pa time i e-mail poruke.

• Poruke koje su dio poslovnog procesa treba arhivirati i čuvati propisani vremenski period kao i dokumente na papiru.

**ANTIVIRUSI**

Virusi i crvi predstavljaju opasnost za informacijske sustave, ugrožavajući funkcioniranje mreže i povjerljivost podataka.

Nove generacije virusa su izuzetno složene i opasne, sposobne da prikriju svoje prisustvo, presreću unos podataka na tipkovnici. Informacije poput zaporki ili povjerljivih dokumenata mogu slati svome tvorcu nekamo na Internet, te otvoriti kriptiran kanal do vašeg računala, kako bi hackeri preuzeli kontrolu nad njim.

Stoga zaštita od virusa ne smije više biti stvar osobnog izbora, već obaveza ustanove, administratora računala i svakog korisnika.

Ustanova propisuje da je zaštita od virusa obavezna i da se provodi na nekoliko razina:

• na poslužiteljima elektroničke pošte

• na internim poslužiteljima, gdje se stavlja centralna instalacija

• na svakom osobnom računalu korisnika

Administratori su dužni instalirati protuvirusne programe na sva korisnička računala i konfigurirati ih tako da se izmjene u bazi virusa i u konfiguraciji automatski propagiraju sa centralne instalacije na korisnička računala u lokalnoj mreži, bez aktivnog sudjelovanja korisnika.

Korisnici ne smiju samovoljno isključiti protuvirusnu zaštitu na svome računalu. Ukoliko iz nekog razloga moraju privremeno zaustaviti protuvirusni program, korisnici moraju

obavijestiti sistem inženjera.

**ADMINISTRATORI i KORISNICI**

Administratori računala svakodnevno prate rad sustava, čitaju dnevničke zapise i provjeravaju rad servisa. Zadaća je administratora i nadgledanje rada korisnika, kako bi se otkrile nedopuštene aktivnosti. Svaka neodgovorna namjerna zlonamjerna aktivnost prijavljuje se i sankcionira privremenim ili stalnim oduzimanjem korisničkih prava u mreži.

Korisnici su dužni odgovorno koristiti računalnu mrežu i ne ugrožavati rad sustava.

Administrator sustava/administrator resursa:

Silvija Jularić

Administrator imenika:

Danijela Begović Jankić

Ravnatelj:

Slavko Kenđelić