Na temelju članka 31. Statuta Tehničke škole Zagreb, na prijedlog ravnatelja, Školski odbor na sjednici održanoj dana 20. siječnja 2016. godine donosi

Odluku o prihvatljivom korištenju računalnih resursa u Tehničkoj školi Zagreb

Uvod

Svrha odluke o prihvatljivom korištenju računalnih resursa u Tehničkoj školi Zagreb (u daljnjem tekstu Škole) je jasno određivanje načina dopuštenog i prihvatljivog korištenja računala i mreža Škole i njihovih usluga.

Cilj odluke o prihvatljivom korištenju računala u školi je definiranje sigurnosnih politika informacijskog sustava Škole te upravljanje tom sigurnošću. Bitno je definirati prihvatljive i neprihvatljive oblike ponašanja prilikom korištenja računalne infrastrukture Škole te raspodijeliti uloge i odgovornosti svih dionika.

Sigurnosna politika

Ljudski i informacijski resursi se smatraju najvažnijim vrijednostima Škole. Stoga je za sigurno rukovanje informacijama potrebno uspostaviti pravila njihova korištenja kao i ponašanja njihovih korisnika. U tom smislu je prihvatljivo korištenje mrežnih i računalnih resursa Škole od iznimne važnosti. S obzirom da rad Škole ovisi i o radu školske infrastrukture, školska računala (i druga školska računalna imovina) moraju biti podešena tako da omoguće neometan pristup i korištenje informacija potrebnih u nastavi i drugim aktivnostima vezanim za rad Škole.

Sigurnosna politika definirana ovim dokumentom vrijede za:

- Cjelokupnu računalnu opremu Tehničke škole Zagreb (oprema školske zgrade, učeničkog doma, školske radionice, prijenosna računala Škole i službenim mobilnim uređajima s mogućnosti pristupa računalnim mrežama, sustav video nadzora u svim objektima)
- Administratora računalne infrastrukture
- Korisnike – zaposlenike Škole i učenike, vanjske suradnike i polaznike edukacija
- Vanjske suradnike za održavanje – tvrtke koje su involvirane u održavanje hardvera ili softvera Škole i video nadzora Škole
- Svako nepridržavanje pravila definiranih ovim dokumentom (sigurnosnih politika) ima negativan utjecaj po Školu i može rezultirati sankcijama. Sankcije izriče Ravnatelj škole (za zaposlenike) i Nastavničko vijeće (pedagoške mjere za učenike). Za vanjske suradnike i polaznike edukacija, vanjske suradnike za održavanje – tvrtke koje su involvirane u održavanje hardvera ili softvera Škole i video nadzora Škole otkazati će se suradnja i poduzeti odgovarajuće pravni

koraci ovisno o mogućoj materijalnoj šteti i zaštiti ugleda Škole i pojedinca (korisnika).

Svako ponašanje protivno ovoj Odluci potrebno je prijaviti odgovornoj osobi (nastavnik ili administrator resursa ili sistem inženjer mreže ili voditelj učionica) ili ravnatelju škole.

Za nepridržavanje ovih pravila posljedice snosi pojedinac koji je postupio protivno odredbama ove Odluke.

U slučaju nastanka materijalne štete provedbu nadoknade štete utvrđuje Ravnatelj.

Sigurnost informacija

Načelo povjerljivosti informacija podrazumijeva da informacije moraju biti dostupne samo onome kome su namijenjene.

U skladu s ovim načelom Škola razlikuje javne i interne informacije.

Skupinu javnih informacija čine one informacije koje opisuju djelatnosti Škole, a njihova javna dostupnost je u interesu Škole. Tu spadaju kontaktni podaci Škole, promidžbeni materijali, internetske stranice Škole, Katalog informacija i sl.

Interne informacije su one informacije koje se odnose na osobne podatke pojedinaca (npr. kontakt podaci osobe, fotografije osobe, podaci iz evidencija koje vodi Škola; Razredna knjiga, Imenik učenika, registri, matične knjige, e-dnevnik, e-matice) te informacije koje su namijenjene samo djelatnicima Škole. Tuđe osobne podatke zabranjeno je koristiti bez dopuštenja osobe odgovorne za te podatke.

S obzirom da je nužno osigurati povjerljivost i sigurnost informacija nužno je:

- Osigurati dostupnost informacije samo onome kome su i namijenjene
- Osigurati laku dostupnost javnih informacija Škole
- Zaštititi interne informacije koje mogu biti dostupne samo uz suglasnost odgovorne osobe
- Zaštititi osobne podatke koji nisu javne informacije
- Osigurati sigurnosne kopije (backup) svih podataka čiji bi gubitak prouzročio štetu
- Fizički zaštititi pristup informacijama važnim za funkcioniranje Škole ili provedbu sigurnosnih politika (zaključavanje sigurnosnih kopija podataka, zaključavanje poslužitelja)

- **Izričito je zabranjeno od učenika, polaznika, učenika smještenih u učeničkom domu, korisnika učeničkog servisa zahtijevati pristupne podatke (elektroničke identitete i pripadne lozinke ili pinove) za pristup e-aplikacijama koje predstavljaju njihove osobne račune.**

- **Da svi nastavnici i zaposlenici Škole dužni su u svojoj poslovnoj komunikaciji koristiti službenu elektroničku adresu (@skole.hr).**

- **Nastavnici i zaposlenici Škole ne smiju vlastite elektroničke identitete i pripadne lozinke ili pinove davati učenicima. To se odnosi na personalizirani pristup: računalu, matici podataka Grada Zagreba, MZOS matici, e-dnevniku, bazi NCVVO-a, bazi za upise u srednje škole, ettaedu.eu sustavu, računovodstvenim programima, programima učeničkog servisa, knjižničarskim programima i ostalim programima ili web aplikacijama koje sadrže osobne podatke zaposlenika i/ili učenika.**

Nastavnici, zaposlenici Škole te vanjski suradnici koji radi prirode posla imaju pristup osobnim podacima ostalih osoba dužni su pridržavati se svih pozitivnih zakona i etičkih načela te o tome potpisati izjavu o „tajnosti podataka“.

Struktura školskih računalnih mreža i definiranje odgovornost o održavanju:

Škola raspolaže računalima, poslužiteljima, računalnom mrežom te video nadzorom.

Škola za održavanje računalne infrastrukture u svojoj odgovornosti može zadužiti djelatnika škole ili angažirati vanjskog suradnika (u daljnjem tekstu Sistem inženjer). Sistem inženjer obvezuje se da sve potrebne pristupne podatke vezane za održavanje mreže ažurno, u osiguranoj omotnici (potpis i pečat Škole) pohranjuje u sefu Škole.

Sigurnost školske računalne mreže

Sigurnost školske računalne mreže preduvjet je provođenja svih drugih sigurnosnih politika informacijskog sustava Škole te je potrebno osigurati sljedeće:

- Osigurati neometanu dostupnost informacija putem računalne mreže u svim prostorima Škole gdje je to potrebno

- Podijeliti računalnu mrežu u dvije fizički odvojene računalne mreže, učeničku i nastavničku. Učenička mreža implementirana je u računalnim kabinetima i u prostoru knjižnice.

- Cijelu računalnu mrežu zaštititi vatrozidom i na njemu dozvoliti uporabu samo osnovnih protokola, te jednosmjernu komunikaciju iz nastavničke u učeničku mrežu

- U računalnoj mreži uspostaviti dvije MS Windows domene, nastavničku i učeničku te na klijentskim računalima omogućiti isključivo autentikaciju u te domene
- Sva serverska računala zaštititi antivirusnim softverom
- Fizički zaštititi serverska računala od neovlaštenog pristupa (ormar sa ključem)
- Poslužitelje zaštititi od nestanka napajanja (UPS zaštita)
- Implementirati zaštitu diskova poslužitelja (RAID 1)
- Dokumentirati stanje mreže i poslužitelja
- Bežičnu mrežu Škole (WIFI) zaštititi od neovlaštenog pristupa (WPA/WPA2). Bežična mreža (WiFi) potrebno je podesiti tako da samo legitimni korisnici mogu pristupiti i koristiti mrežu. Legitimni korisnici mogu biti nastavno i administrativno tehničko osoblje te učenici.
- Vanjski pristup računalnoj mreži Škole osigurati isključivo preko VPN konekcije. To je potrebno omogućiti isključivo putem sigurnih protokola. Neki servisi koji koriste sigurne protokole i koje se preporuča koristiti za spajanje na školska računala s Interneta su SSH v.2 servis, web sučelje koje omogućuje prijavu korisnika a koristi isključivo HTTPS protokol ili VPN.

Dokumentacija izgleda mreže 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.

U cilju održavanja visoke razine sigurnosti računalne mreže nužno je pratiti nova tehnološka rješenja koja odgovaraju zahtjevima. Računalnu mrežu potrebno je redovito održavati i razvijati.

Škola, CARNet i CERT zadržavaju pravo nadzora i filtriranja mrežnog prometa.

Škola može zatražiti od CARNeta, odnosno MZOS-a reviziju filtriranog sadržaja.

Sigurnost školskih računala

Ispravna konfiguracija računala olakšava njihovo održavanje, a ujedno i povećava sigurnost učenika i nastavnika odnosno ostalih zaposlenika škole. Zato je potrebno da sva računala u školi imaju minimalni skup preporučenih sigurnosnih postavki.

U cilju provođenja sigurnosnih politika na klijentskim računalima nužno je:

- Redovito održavanje sustava kroz preuzimanja svih ažuriranja softvera (uključiti Windows Update)

- Instalirati isključivo softver koji je nužan i za koji škola posjeduje odgovarajuće licence
- Na svim klijentskim računalima uključiti vatrozid
- Osigurati autentikaciju na računala koja svakome korisniku osigurava odgovarajuća prava (kroz MS Windows Active Directory)
- Onemogućiti korisnicima administriranje računala. Korisnici zahtjeve za administriranjem računala prosljeđuju administratoru školske mreže
- Na svim računalima implementirati antivirusnu zaštitu (Sophos Antivirus, MS Forefront Endpoint Protection)
- Dokumentirati stanje hardvera i softvera na svakom pojedinom računalu
- Kroz upotrebu mrežnih mapa osigurati korisnicima veću sigurnost podataka i olakšani pristup podacima
- Ukoliko netko koristi nelegalan softver ili softver koji je instalirao bez dozvole Sistem inženjera za sve štete osobno snosi krivicu. Sistem inženjer ili druga odgovorna osoba nisu dužni sanirati štete nastale korištenjem neovlašteno instaliranog softvera.
- Računala koja se spajaju na WiFi mreže eduroam i e-dnevnik moraju biti podešena tako da prije početka rada traže prijavu korisnika autentikacijom putem AAI sustava.
- U prostorima škole u kojima se nalazi računalna oprema učenici mogu biti isključivo uz nazočnost nastavnika
- Učenici na računala ne smiju samostalno instalirati nikakve korisničke programe.

Sigurnost korisnika

Infrastruktura škole mora svim svojim korisnicima pružiti neometan i siguran pristup informacijama, svugdje gdje je to potrebno. Međutim, sigurnost korisnika ovisi i o njihovom znanju i ponašanju.

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 i nastavnika te ostalih zaposlenika o sigurnosnim aspektima prilikom korištenja računala i mobilnih uređaja.

- Korisnicima osigurati autentikaciju na klijentska računala sa odgovarajućim pravima u računalnom sustavu

- Svi korisnici školskih računala moraju se prijaviti na sustav prije korištenja i odjaviti nakon završetka korištenja.
- Kod pristupa nekim aplikacijama potrebno je korištenje certifikata odnosno pametne kartice koji jednoznačno i vjerodostojno identificiraju korisnika ili kombinacije pina i jednokratne lozinke (token).
- Korisnicima pružiti odgovarajuću edukaciju o sigurnom korištenju računala
- Korisnici su obvezni čuvati svoje korisničke podatke, te nakon završenog rada odjaviti se sa računala, servisa ili baze podataka
- Korisnici ne smiju koristiti tuđe korisničke podatke. U iznimnom slučaju da je to potrebno zbog obavljanja radnih zadaća, nužno je tražiti suglasnost osobe čiji pristupni podaci se koriste te suglasnost ravnatelja. Osoba koja je (iz objektivnih razloga) dala svoje pristupne podatke na korištenje mora što prije promijeniti svoje pristupne podatke.
- Korisnici su dužni svaku uočenu neispravnost u radu računala ili sustava odmah prijaviti administratoru
- Prava pristupa učenika i zaposlenika škole školskim računalima potrebno je redovito provjeravati i po potrebi mijenjati, minimalno jednom godišnje
- Početkom školske godine potrebno je revidirati i elektroničke identitete (AAI) učenika.
- Učeniku je potrebno ukinuti prava pristupa školskim računalima i isključiti školske elektroničke identitete najkasnije 1. listopada u godini u kojoj je završio školovanje, odnosno danom ispisa iz škole za učenike koji se ispisuju iz škole prije završetka školovanja.
- Zaposleniku Škole potrebno je ukinuti prava pristupa školskim računalima i isključiti sve školske elektroničke identitete danom isteka ugovora o radu u Školi. Iznimno, uz odluku Ravnatelja, moguće je produljiti valjanost školskih elektroničkih identiteta zaposleniku i nakon prestanka radnog odnosa u Školi, a radi dovršavanja već započetih poslova.
- Učenici smiju koristiti samo školska računala namijenjena njima. Vlastita računala i pametne telefone tijekom nastave učenici smiju koristiti isključivo u obrazovne svrhe uz prethodnu dozvolu nastavnika.
- Učenici smiju koristiti školska računala u privatne svrhe isključivo u slobodno vrijeme (za vrijeme odmora, te prije ili nakon nastave) u knjižnici škole i učionici doma.

- Učenici koriste školska računala unutar računalnih učionica s korisničkim računom koji odredi nastavnik. Nastavnik koji koristi računalnu učionicu dužan je za svaki nastavni sat imati točan raspored sjedenja pojedine razredne grupe. Popis je dio nastavničke dokumentacije.

- Učenici borave u računalnoj učionici u prisutnosti nastavnika. U informatičkoj učionici nije dozvoljeno konzumiranje jela i pića. Ukoliko učenik primijeti neki kvar (hardverski ili softverski) o tome treba odmah obavijestiti nastavnika. Učenicima nije dozvoljeno samovoljno „popravljanje“ računala.

- Korisnici su obvezni voditi računa o tome da svojim radom u računalnoj mreži ne ugrožavaju sebe, druge korisnike i podatke (antivirusna provjera podataka na prijenosnim memorijama, prosljeđivanje e-mail poruka, slanje masovnih e-mail poruka, posuđivanje svojih korisničkih podataka drugim korisnicima)

- Korisnici su obvezni čuvati podatke, tokene i kartice koje koriste za pristup računalima i programima tajnima. Korisnici ne smiju koristiti tuđe pristupne podatke za korištenje računala.

Politika prihvatljivog korištenja informacijsko komunikacijskih tehnologija

Korištenjem informacijskih tehnologija u Školi osigurava se jednostavan pristup informacijama, dijeljenje informacija te se obogaćuje nastavni proces upotrebom edukacijskog softvera, servisa na mreži i multimedijalnih materijala.

Korisnici moraju znati da sadržaji koji se nalaze na Internetu ne moraju biti istiniti. Činjenice koje se pronalaze na Internetu moraju se koristiti s oprezom ukoliko nisu provjerene. Učenici trebaju koristiti informacije s Interneta u skladu s uputama nastavnika. Sadržaji koji se koriste za nastavu moraju se koristiti iz provjerenih izvora.

Ukoliko korisnik primijeti neprimjerene, uznemirujuće ili sadržaje koji ugrožavaju njihovu sigurnost, o tome odmah trebaju obavijestiti svog nastavnika, voditelja, stručnog suradnika škole ili ravnatelja.

Korisnici računalne infrastrukture Škole moraju se ponašati odgovorno te prihvatiti politike prihvatljivog korištenja računala:

- Korisnici su odgovorni za sadržaje koje objavljuju. I privatna aktivnost u računalnoj mreži može bitno narušiti njihov ugled i ugled Škole

- Zabranjeno je vrijeđanje, omalovažavanje drugih korisnika mreže te objava neprimjerenih sadržaja

- Korisnik treba svojim potpisom stajati iza sadržaja koji objavljuje

- Korisnik može objavljivati tuđe materijale samo uz privolu autora ili ako se radi o materijalu koji se slobodno može preuzimati (npr. Creative Commons). Korištenje tuđih materijala s Interneta mora biti citirano uz navođenje autora
- Korisnici su dužni na odgovarajući način zaštititi svoju i tuđe privatnosti u mreži. Jednom objavljene podatke na Internetu gotovo je nemoguće maknuti sa mreže.
- Korisnici moraju uvijek imati kritički pristup podacima koje preuzimaju sa Interneta
- Zabranjeno je preuzimanje autorski zaštićenih datoteka ili softvera bez plaćanja naknade
- Društvene mreže korisnici moraju koristiti isključivo za poticanje suradnje, međusobnog pomaganja, a nikako suparništva i rivalstva
- Zabranjeno je korištenje tuđeg identiteta
- Zabranjeno je provaljivanje na druga računala u mreži te istraživanje njihove ranjivosti
- Zabranjeno je slanje masovnih poruka
- Zabranjeno je korištenje P2P softvera (razni torrent klijenti) te korištenje proxy-ja u svrhu zaobilaženja ograničenja u lokalnoj mreži Škole

Ova odluka bit će objavljena na oglasnoj ploči Tehničke škole Zagreb, te stupa na snagu danom donošenja.

KLASA: 602-03/16-10/44

URBROJ: 251-113-16-10-2

Zagreb, 20. siječnja 2016.

Predsjednik Školskog odbora	**Ravnatelj**
Bože Antunović	Darko Jurković