PRAVILNIK O INFORMACIJSKOJ SIGURNOSTI

U Slavonskom Brodu, prosinac 2018.

Sadržaj:

1. UVOD

Ovim Pravilnikom uređuju se pravila postupanja u OSNOVNOJ ŠKOLI HUGO BADALIĆ, BOROVSKA 3), Slavonski Brod (dalje u tekstu: Škola) glede informacijske sigurnosti. Kako bi osigurala uspješno obavljanje poslova iz svojeg djelokruga, Škola prepoznaje potrebu da poslovanje Škole teče glatko i bez prekida, stoga su informacijska sigurnost, odnosno osiguranje povjerljivosti, integriteta i raspoloživosti podataka koja Škola obrađuje te zaštita informacijske imovine sastavni dio svih poslovnih procesa Škole.

Glavni ciljevi informacijske sigurnosti su sljedeći:

- očuvanje prihvatljive razine rizika informacijske sigurnosti;
- zaštita podataka od neovlaštene ili nezakonite obrade, gubitka, uništenja ili oštećenja;
- stvaranje povjerenja kod roditelja djece koja pohađaju Školu i poslovnih partnera Škole u sigurnost podataka koji su povjereni Školi;
- osiguranje podrške zahtjevima regulatornih tijela po pitanju sigurnosti podataka;
- prevencija moguće štete zbog gubitka, oštećenja, zloupotrebe ili otuđenja podataka.

Specifični ciljevi informacijske sigurnosti utvrđuju se na osnovi rezultata procjene rizika i postižu implementacijom tehničkih, proceduralnih i organizacijskih kontrola u skladu s planovima otklanjanja i/ili umanjenja rizika.

Kako bi se osigurala potrebna razina zaštite, Škola je implementirala skup kontrola informacijskog sustava s ciljem da se otklone percipirani rizici informacijske sigurnosti.

2. DEFINICIJE

Za potrebe Pravilnika sljedeći pojmovi će imati značenje kako slijedi:

Pojam	**Značenje**
Informacijski sustav Škole	skup svih podataka, informacija i dokumentacije koje Škola obrađuje na temelju valjane pravne osnove, neovisno na kojem mediju su zapisani;
Informatički sustav Škole	sva informatička oprema u vlasništvu Škole ili u upotrebi od strane Škole;
Podaci	svi podaci koji se nalaze ubilježeni na bilo kojem mediju ili u bilo kojem obliku te se obrađuju od strane Škole;
Pristup	Mogućnost uvida, preuzimanja, izmjene ili brisanja podataka;
Rizik informacijske sigurnosti	Kombinacija vjerojatnosti nastanka događaja narušavanja informacijske sigurnosti i posljedica takvog događaja na izvršavanje poslovnih procesa;
Mobilni uređaj	Laptop, tablet, mobitel ili sličan uređaj;

3. KONTROLA PRISTUPA INFORMACIJAMA

Podaci koji su dio informacijskog sustava čine se zaposlenicima dostupnima u skladu s potrebama njihovog radnog mjesta.

Podaci zabilježeni u fizičkom obliku čuvaju se ograničenjem pristupa te nadzorom ulaska u prostorije u kojima su podaci pohranjeni (odnosi se na sve radne prostorije u kojima se pohranjuju podaci, ne samo arhivu). Ulazak u prostorije u kojima su podaci pohranjeni dopušten je samo osobama koje rade u tim prostorijama te osobama koje imaju ovlaštenje za ulazak u prostorije. Posjetitelji, vanjski suradnici i poslovni partneri mogu ući u radne prostorije isključivo uz prisutnost ovlaštenog zaposlenika Škole.

Podaci se pohranjuju na sigurnom mjestu (u zaključanom ormaru i/ili u zaključanoj prostoriji) u skladu s propisima koji uređuju čuvanje dokumentarnog gradiva (Zakon o arhivskom gradivu i arhivima).

Nije dopušteno iznošenje Podataka, Mobilnih uređaja na kojima su isti pohranjeni niti oprema koja predstavlja Informatički sustav Škole bez dopuštenja odgovorne osobe.

Zaposlenici će u obavljanju svojih radnih zadataka primjenjivati „politiku čistog stola“. U navedeno spadaju posebno sljedeće mjere:

- sve povjerljivi ili osjetljivi podaci moraju biti uklonjene sa stola i zaključane u ormar ili u posebnu, za to namijenjenu prostoriju, kada je stol prazan i na kraju radnog dana;
- ormari i prostorije s dokumentima koji sadrže povjerljive ili osjetljive podatke moraju biti zatvoreni i zaključani kada nisu u upotrebi. Ključevi se ne smiju ostavljati u vratima ormara;
- računalne radne stanice moraju biti zaključane kada je radni prostor prazan;.
- računalne radne stanice moraju biti potpuno zatvorene na kraju radnog dana;
- zaporke se ne smiju ostavljati na ljepljivim bilješkama postavljene na ili ispod računala, niti ih smiju biti zapisane na lako vidljivim i pristupačnim mjestima.

U praksi se mogu koristiti i druge potrebne mjere.

4. KONTROLA PRISTUPA INFORMATIČKOM SUSTAVU

Inicijalno je svaki pristup informatičkom sustavu zabranjen (onemogućen osobama koje nisu ovlašteni korisnici). Početna prava za pristup informatičkom sustavu korisnicima (zaposlenicima) se dodjeljuju sukladno zahtjevima poslovnih procesa u kojima sudjeluju. Sva dodatna prava pristupa resursima informatičkog sustava dokumentiraju se i moraju biti utemeljena na poslovnoj potrebi, tj. korisnicima se pristup mora eksplicitno dodijeliti za one resurse informatičkog sustava koji su im potrebni za obavljanje radnih zadataka.

Svaki korisnik prilikom pristupa sustavu mora se identificirati upotrebom korisničkog imena radi provjere ovlaštenja. Pored korisničkog imena kojim pristupa sustavu svaki korisnik dobiva i zaporku kao dio mehanizma autentifikacije. Korisnik informatičkog sustava je odgovoran za čuvanje tajnosti svojih zaporki.

Sve dodijeljene ovlasti i korisnički računi revidirat će se uslijed svake značajne promjene u sustavu, a najmanje jednom godišnje.

Sva informatička oprema mora biti evidentirana i svi korisnici uredno zabilježeni.

5. PRAVILA O ANTIVIRUSNOJ I MALWARE ZAŠTITI

Kako bi se spriječila infekcija Informatičkog sustava Škole i izbjegle potencijalno teške posljedice takve infekcije, Škola će postaviti niz odgovarajućih mjera zaštite. S obzirom na složenost i nepredvidivost mogućih ugroza, kako bi se osigurala zaštita podataka nije dovoljno osloniti se samo na jednu mjeru, već je potrebno sustavno primijeniti niz različitih mjera (načelo slojevitog pristupa zaštitnim mjerama). Mjere koje se primjenjuju su kako slijedi:

5.1. Vatrozid (Firewall)

Vatrozid će biti instaliran na svim mjestima na kojima je interna mreža povezana s internetom. Dozvole pristupa moraju biti postavljene tako da korisnik ne može onemogućiti vatrozid.

5.2. Antvirusna zaštita

Komercijalna i podržana antivirusna platforma će se instalirati na ključnim lokacijama:

- vatrozidu;
- poslužiteljima e-pošte;
- proxy poslužiteljima;
- svim ostalim poslužiteljima;
- svim korisničkim računalima;
- Mobilnim uređajima.

Svi protuvirusni programi bit će postavljeni tako da se redovito ažuriraju. U zadanim postavkama protuvirusnih programa, prilikom skeniranja pristupa mora biti omogućeno pružanje zaštite u stvarnom vremenu. Redovita puna skeniranja moraju se provesti najmanje jednom tjedno.

Korisnici ne smiju onemogućiti antivirusnu zaštitu na uređajima koje koriste.

5.3. Filtriranje neželjenih podataka

U Informatičkom sustavu Škole instalirat će se sustav za filtriranje neželjenih i potencijalno štetnih poruka e-pošte (neželjene pošte). Filtriranje mora osigurati da vrste privitaka koji često sadrže zlonamjerni softver budu blokirane ili uklonjene prije isporuke korisniku.

5.4. Instalacija i skeniranje softvera

Korisnici Informatičkog sustava Škole ne smiju imati takav administrativni pristup istome koji bi omogućio instaliranje nedopuštenog softvera. Na svim dijelovima Informatičkog sustava Škole dopušteno je korištenje smo licenciranog software-a, a IT služba će software instalirati samo na temelju odgovarajućeg naloga odgovorne osobe. Skeniranje Informatičkog sustava Škole s ciljem otkrivanja neovlaštenog software-a provoditi će se na redovitoj osnovi.

5.5. Upravljanje ranjivostima

Informacije o ranjivosti software-a prikupit će se od dobavljača software-a, odnosno, po potrebi od trećih strana te će se, tamo gdje je to moguće, ažuriranja automatski primjenjivati. Skeniranje ranjivosti mora se redovito provoditi.

5.6. Obuka korisnika

Zaposlenici Škole će se, kao korisnici Informatičkog sustava Škole, po stupanju na snagu Pravilnika informacijske sigurnosti odnosno prije početka korištenja sustava, upoznati s Pravilnikom informacijske sigurnosti i najčešćim rizicima.

6. POSLOVNI PARTNERI

Škola će utvrditi rizike za informacijsku sigurnost te poduzimati zaštitne mjere s ciljem otklanjanja ili smanjenja rizika.

U poslovnim odnosima u kojima dolazi do razmjene osobnih podataka, Škola će s poslovnim partnerima sklopiti sporazum o obradi osobnih podataka kojim će se specificirati sigurnosni zahtjevi glede obrade osobnih podataka.

7. PRAVILA O UPOTREBI MOBILNIH UREĐAJA

Svrha Pravila o upotrebi mobilnih uređaja je odrediti kontrole koje moraju biti postavljene prilikom korištenja Mobilnih uređaja. Namjera je ublažavanje sljedećih rizika:

- gubitka ili krađe Mobilnih uređaja, uključujući podataka u njima;
- neželjenog otkrivanje povjerljivih podataka putem korištenja u javnosti;
- unošenja virusa i zlonamjernog softvera u Informacijsku mrežu Škole;
- gubitka ugleda Škole.

Škola će voditi ažurnu evidenciju korisnika Mobilnih uređaja u poslovne svrhe.

Mobilni uređaj dan zaposleniku na korištenje od strane Škole treba se koristiti se isključivo za obavljanje poslova iz djelokruga Škole i to samo od strane korisnika kojemu je isti dodijeljen; nije namijenjen za dijeljenje s bilo kojim trećim osobama niti za osobne aktivnosti. Mobilni uređaj je vlasništvo Škole i od zaposlenika se u bilo kojem trenutku može tražiti da isti vrati ili da ga dostavi na pregled.

Na Mobilnom uređaju nije dopušteno instalirati neovlašteni softver, mijenjati konfiguraciju uređaja ili priključivati periferni hardver bez prethodnog odobrenja IT službe Škole.

Mobilni uređaj se treba koristiti tako da se štiti od oštećenja te se također treba prenositi u zaštitnom kućištu kad god je to moguće. Gdje je to moguće, Mobilni uređaj će biti osiguran tako da su svi podaci u njemu šifrirani i stoga dostupni samo ako je korisniku poznata zaporka. Ako je Mobilni uređaj isporučen s enkripcijom, ista se ne smije onemogućiti.

Mobilni uređaj se ne smije ostavljati bez nadzora u javnom prostoru (npr. sobi za sastanke, automobilu). Tokeni za pristup, korisničko ime i zaporka ili drugi sigurnosni predmeti se ne bi trebali držati zajedno sa uređajem. U slučaju gubitka Mobilnog uređaja, bez odgode treba obavijestiti neposredno nadređenu odgovornu osobu u Školi i IT službu Škole.

Gdje je to moguće, Škola će na Mobilni uređaj ugraditi zaštitu od virusa. Nije dopušteno onemogućavati zaštitu od virusa na Mobilnom uređaju.

Nije uputno povezivati Mobilni uređaj s nezaštićenim javnim mrežama, osim ako se ne koristi VPN (Virtual Private Network). Kada se koristi na javnim mjestima, potrebno je Mobilni uređaj koristiti tako da neovlašteni korisnici ne mogu gledati (ili snimati fotografije ili videozapise) zaslona.

S posljednjim danom radnog odnosa zaposlenika ili s danom zaduživanja zamjenskog uređaja, zaposlenik je dužan vratiti Mobilni uređaj Školi.

Nije dopušteno korištenje vlastitih uređaja zaposlenika za poslovne svrhe. Pod korištenjem Mobilnih uređaja u smislu ovog Pravilnika ne smatra se korištenje osobne imovine (uređaja) zaposlenika.

8. PRIMJENA PRAVILNIKA O INFORMACIJSKOJ SIGURNOSTI

Sadržaj Pravilnika o informacijskoj sigurnosti pregledan je i odobren od strane Škole te je primjena Pravilnika obvezna u obavljanju poslova iz djelokruga Škole. Nepridržavanje zahtjeva iz Pravilnika o informacijskoj sigurnosti od strane zaposlenika smatra se povredom obveza iz ugovora o radu.

9. ZAŠTITA OSOBNIH PODATAKA

Zaštita osobnih podataka uređena je Politikom o zaštiti osobnih podataka.

10. AŽURIRANJE PRAVILNIKA O INFORMACIJSKOJ SIGURNOSTI

Pravilnik o informacijskoj sigurnosti treba se provjeravati i usklađivati s rezultatima provjere sustava upravljanja informacijskom sigurnošću te promjenama u organizacijskom okruženju, poslovnim prilikama, zakonskim propisima i tehnologijama uslijed kojih je potrebna njena prilagodba i poboljšanje. Za provjeru i ažuriranje Pravilnika odgovorna je osoba koju Škola za to zaduži.

Ovaj Pravilnik stupa na snagu danom donošenja, a primjenjuje se protekom roka od osam dana od dana objave.

KLASA: 011-03/18-01/04
URBROJ: 2178/01-04-01-18-1
Slavonski Brod, 20. prosinca 2018.g.

RAVNATELJICA: PREDSJEDNICA ŠKOLSKOG ODBORA

_____ _____