Temeljem članka 18. Zakona o zaštiti osobnih podataka i članka 79. Statuta Visoke škole za sigurnost, dana 13.5.2018. dekan Škole donio je:

PRAVILNIK

O SIGURNOSTI INFORMACIJSKOG SUSTAVA

Temeljne odredbe

Članak 1.

Pravilnikom o sigurnosti informacijskog sustava (dalje u tekstu: Pravilnik) definiraju se uvjeti korištenja informacijskog sustava Visoke škole za sigurnost (dalje u tekstu: Škola), raspolaganje i uvjeti korištenja računalne, telekomunikacijske i programske opreme, prava i obveze korisnika, mjere održavanja i provjere ispravnosti rada, sredstva i uvjeti pohranjivanja podataka, osiguranje radnih prostorija u kojima je smještena ta oprema, mjere sigurnosti i zaštite sustava te osobe ovlaštene za provedbu predviđenih mjera.

Članak 2.

Pojmovi za potrebe ovog Pravilnika imaju sljedeće značenje:

- *Korisnik* je svaka fizička osoba koja pristupa računalnoj mreži ili koja koristi programsku podršku ili poslovne baze podataka na računalnoj opremi Škole.

- *Korisničko ime* (isto što i log in, account name, user name i slično) je skraćeno ime korisnika definirano na računalu, pojedinim programima ili na sustavu, a služi za pristup pojedinim resursima informacijskog sustava.
- *Korisnički račun* je skup koji se sastoji od korisničkog imena i lozinke s točno definiranim pravima za rad na računalu, pojedinim programima ili na sustavu.
- *Dijeljena mapa* (folder) je mapa korisnika ili grupe korisnika kojima je dodijeljeno pravo pristupa istoj, služi za pohranu i razmjenu elektroničkih dokumenata.
- *Administrator sustava* je osoba zadužena za tehničko održavanje računala, pojedinih programa ili sustava.
- *Programska podrška* je skup svih računalnih programa potrebnih za rad i kontrolu računalnih sustava te skup svih sistemskih, operativnih, uslužnih i aplikativnih programa.

- *Poslovne aplikacije* su programi koji služe za vođenje pojedinih poslovnih procesa unutar informacijskog sustava.
- *Računalna oprema* podrazumijeva računala i druge elektroničke uređaje za pohranu, obradu, prijenos i prikaz podataka.
- *Adresa elektroničke pošte je* isto što i e-mail adresa, jedinstvena adresa korisnika koja se korisnicima otvara za potrebe obavljanja radnih zadataka i poslovnih procesa te poslovnog komuniciranja; vezana je uz korisnički račun.
- *Privitak* je isto što i ''attachment'', dokument koji je u obliku datoteke poslan putem elektroničke pošte.
- *Informacijski sustav* je komunikacijski, računalni ili drugi elektronički sustav u kojem se podaci obrađuju, pohranjuju ili prenose, tako da budu dostupni i upotrebljivi za ovlaštene korisnike.

- *Mjere informacijske sigurnosti* su opća pravila zaštite podataka koja se realiziraju na fizičkoj, tehničkoj ili organizacijskoj razini.

Opseg primjene

Članak 3.

Ovaj Pravilnik odnosi se na zaposlenike, vanjske suradnike i studente. U daljnjem tekstu termin korisnik odnosit će se na sve osobe kojima se dopušta uporaba računalnog informacijskog sustava Škole.

Pravilnik obuhvaća računalni informacijski sustav Škole i sve sadržaje koji se prenose, pohranjuju i obrađuju u tom sustavu, sadržaje pohranjene na svim računalima u vlasništvu Škole, kao i sve poslužitelje koji su u administrativnoj domeni ili vlasništvu Škole.

Odgovornost

Članak 4.

Za primjenu ovog Pravilnika i korištenje informatičke opreme u vlasništvu Škole odgovoran je dekan Škole (u daljnjem tekstu: dekan).

Za tehničku podršku računalnog informacijskog sustava Škole odgovoran je administrator sustava. Administratora sustava imenuje dekan iz redova nastavnika.

Administrator sustava zadužen je i odgovoran za:

- administriranje i održavanje sigurnosti računalnog informacijskog sustava, što uključuje materiju koju uređuje ovaj Pravilnik i sve pridružene procedure

- razvijanje i održavanje pisanih standarda i procedura kojima se osigurava primjena i pridržavanje odredbi ovog Pravilnika i procedura
- pružanje odgovarajuće podrške korisnicima u ispunjavanju njihove obveze u odnosu na ovaj Pravilnik i pripadajuće procedure.

Svi korisnici obvezni su proučiti i primjenjivati odredbe ovog Pravilnika, kao i njemu pridružene procedure.

Upravljanje informacijskim sustavom

Članak 5.

Upravljanje informacijskim sustavom Škole u isključivoj je nadležnosti administratora sustava i ugovorenih vanjskih davatelja usluga održavanja računalne mreže.

Administrator sustava vodi dokumentaciju o informacijskom sustavu, koja se obvezno treba čuvati u metalnom ormaru (kasi) u vrijeme kad se ne koristi.

Povjerljivost i integritet podataka pohranjenih na računalnom informacijskom sustavu Škole moraju biti zaštićeni sustavom kontrole pristupa kako bi se osiguralo da samo ovlašteni korisnici imaju pristup pohranjenim podacima.

Pristup treba biti ograničen na samo one informacijske sustave i baze podataka koje su korisniku nužne za njegove poslovne aktivnosti.

Članak 6.

Uvjeti i pravila korištenja informacijskog sustava:

1. Gosti i poslovni partneri ne smiju koristiti informacijski sustav Škole na kojem se nalaze poslovne aplikacije i baze podataka. Iznimka su osobe kojima je pristup sustavu potreban radi obavljanja poslova od značaja za informacijsko-komunikacijski sustav, osobe koje održavaju, ispravljaju nedostatke ili nadograđuju informacijsko-komunikacijski sustav te osobe koje imaju ovlast nadzora, inspekcije ili drugih vidova kontrole pojedinih poslovnih procesa za koje se koristi odgovarajuća programska podrška.

Odobrenje za pristup informacijsko-komunikacijskoj infrastrukturi u ovakvim slučajevima daje dekan. Osoba koja dobije odobrenje za rad na računalu u mreži Ustanove mora prethodno potpisati izjavu o povjerljivosti.

2. Korisnici informacijski sustav smiju koristiti koristeći računalnu opremu konfiguriranu prema uputama administratora sustava. Privatnom opremom (uključujući i mobilne uređaje) korisnici mogu pristupati informacijskom sustavu samo uz odobrenje dekana.

3. Informacijski sustav (računalna mreža) smije se koristiti samo za potrebe poslova koje korisnik obavlja u okviru svojih radnih zadataka i poslovnih procesa.

4. Korisnik koji tijekom rada povrijedi neko od pravila ovog Pravilnika ili učini pogrešku koja ima štetne posljedice za druge osobe ili Školu, obvezan je odmah o tome izvijestiti onoga tko je oštećen, a zatim i administratora sustava.

5. Dekan u slučaju narušavanja sigurnosti informacijskog sustava može privremeno ili trajno korisniku uskratiti pristup informacijskom sustavu Škole.

6. Osim odredbi ovog Pravilnika, za pojedine procese informacijskog sustava mogu biti propisane dodatne upute ili procedure koji predstavljaju nadopunu ovog Pravilnika.

Ispravnost računalne opreme i programska podrška

Članak 7.

Priključenje računalne, telekomunikacijske i druge opreme informacijskog sustava na energetsku mrežu obavlja se prema uputama proizvođača te opreme, u skladu s važećim tehničkim normama.

Računala za vođenje zbirki osobnih podataka priključuju se na energetsku mrežu preko uređaja za neprekinuto napajanje.

Računala za vođenje zbirki osobnih podataka smješta, postavlja i ugrađuje stručna osoba uz odobrenje dekana, u skladu s važećim normama, standardima i tehničkim uputama.

Administrator sustava vodi brigu o tehničkoj ispravnosti sustava, predlaže mjere za njegovo poboljšanje, uključujući nabavu opreme, organizaciju edukacije korisnika i davatelja usluga.

Administrator sustava odgovoran je da sva, za redovito poslovanje nužna, računalna oprema bude priključena na izvore neprekidnog napajanja, a da ostala oprema bude zaštićena prednaponskom zaštitom.

Administrator sustava odgovoran je za sve instalacije, odspajanja, promjene i premještanje računalne opreme. Korisnici ne smiju samostalno poduzimati takve radnje.

Računala se moraju konfigurirati na taj način da budu zaštićena od napada izvana i iznutra, što se osigurava instaliranjem softverskih zakrpi po preporukama proizvođača, listama pristupa, filtriranjem prometa i drugim sredstvima.

Administrator je dužan instalirati antivirusne programe na sva korisnička računala i konfigurirati ih tako da se izmjene u bazi virusa i u konfiguraciji automatski apliciraju sa središnje instalacije na korisnička računala u lokalnoj mreži, bez aktivnog sudjelovanja korisnika.

Posebnu pažnju administrator sustava dužan je posvetiti opremi koja obavlja ključne funkcije ili sadrži vrijedne i povjerljive informacije koje treba štiti od neovlaštenog pristupa (npr. serveri, mrežna oprema i slično).

Davatelji usluga dužni su u svome radu poštivati privatnost ostalih korisnika i povjerljivost informacija s kojima dolaze u dodir pri obavljanju posla.

Administriranje korisnika

Članak 8.

Za kreiranje i zatvaranje korisničkih računa, odnosno za promjenu pojedinih ovlasti i prava na razini operativnog sustava te za kreiranje, zatvaranje i promjenu pojedinih ovlasti za rad s poslovnim aplikacijama i bazama podataka zadužen je administrator sustava.

Administrator sustava odgovoran je za administraciju kontrole pristupa u informacijski sustav, što uključuje dodavanje, brisanje i promjene prava pristupa korisnicima.

Korisnička prava pristupa informacijskom sustavu ostvaruju se nakon odobrenja dekana Škole. Zahtjev se dostavlja putem obrasca ''Zahtjev za administraciju korisnika'', koji je sastavni dio ovog Pravilnika.

Svaki korisnik obvezno mora pristupiti informacijskom sustavu i računalima Škole isključivo vlastitim pristupnim računom.

Administrator sustava može na zahtjev dekana odobriti korisniku korištenje pristupnog računa druge osobe za pronalaženje i otklanjanje nepravilnosti rada sustava, o čemu treba napraviti pisani izvještaj.

Članak 9.

Korisnik računalnog informacijskog sustava Škole:

- odgovoran je za sve računalne transakcije učinjene korištenjem dodijeljenog mu prijavnog imena i zaporke
- ne smije njemu dodijeljene zaporke otkriti drugim osobama
- treba odmah promijeniti svoju zaporku, ako ju je izgubio ili sumnja da ju je netko drugi saznao

- ne smije bilježiti zaporke na lako dostupnom mjestu
- treba često mijenjati zaporke, a obvezno nakon 90 dana korištenja
- treba koristiti zaporke koje nije lako pogoditi
- treba se odjaviti iz informacijskog sustava kada napušta radno mjesto.

Članak 10.

Administrator sustava obvezan je pohraniti sve administratorske zaporke u adekvatni metalni ormar (kasu), koji treba uvijek držati zaključanim.

Pohranjene zaporke trebaju biti u svaka u zasebnoj zapečaćenoj kuverti, na kojoj treba pisati za koji je računalni sustav ili računalnu opremu te datum kad je zadnji puta ažurirana.

Administrator sustava obvezan je redovito nakon svake promjene ažurirati pohranjene zaporke.

Prava i obveze korisnika

Članak 11.

Korisnici su se tijekom korištenja informacijskog sustava dužni pridržavati sljedećih pravila:

1. Korisnik računala nije vlasnik računala nego se njime, kao opremom koja je u vlasništvu Škole služi u okviru posla koji obavlja. Korisnik računala ne može istodobno biti i njegov administrator.

2. Svaki korisnik za rad s računalnom opremom, s razine operacijskog sustava, posjeduje svoje vlastito korisničko ime i lozinku. Anonimne aktivnosti u korištenju sustava nisu dozvoljene.

3. Svaki korisnik poslovnim aplikacijama koje koriste poslovne baze podataka pristupa vlastitim korisničkim imenom i lozinkom koju mu, uz odobrenje dekana, dodjeljuje administrator sustava.

4. Korisnik je odgovoran za sve aktivnosti unutar računalne opreme te poslovnih aplikacija koje su obavljene s njegovim korisničkim imenom.

5. Prilikom privremenog napuštanja radnog mjesta korisnik je dužan onemogućiti da se računalnoj opremi može pristupiti uporabom njegovog korisničkog imena.

6. Prilikom duljeg napuštanja radnog mjesta korisnik je dužan ugasiti računalnu opremu. Korisnik je dužan ugasiti računalnu opremu na kraju radnog dana.

7. Svoje korisničko ime i lozinku korisnik ne smije ustupati drugim osobama, a niti se u svom radu smije koristiti korisničkim imenom i lozinkom koji mu nisu dodijeljeni. Iznimno, ako to nalaže potreba posla, uz prethodnu pisanu suglasnost dekana, korisnik će ustupiti na korištenje svoje korisničko ime i lozinku ili će za rad koristiti tuđe korisničko ime i lozinku. Dekan je dužan osigurati da tijekom njegovog korištenja ne dođe do zloupotrebe. U tom slučaju odgovornost za sve postupke nastale kao posljedica korištenja tuđeg korisničkog imena i lozinke snosi dekan.

8. Odmah po prestanku potrebe korištenja tuđeg korisničkog imena i lozinke, korisnik čije je ime bilo korišteno mora promijeniti lozinku. Ako on to nije u mogućnosti, dekan je dužan od administratora sustava zatražiti izmjenu lozinke.

9. Nije dozvoljeno postavljanje dodatnih programskih podsustava na računalnu opremu kao niti izmjene postavki operacijskog sustava od strane korisnika ili drugih neovlaštenih osoba bez suglasnosti administratora sustava.

10. Računalna oprema koristi se za poslovne procese korisnikovog radnog mjesta.

11. Nije dozvoljen pristup podacima na računalnoj opremi za koju korisnik nema ovlaštenje.

12. Udaljeni pristup do računalne opreme uporabom računalnih mreža može se korisniku dozvoliti samo u iznimnim situacijama (npr. radi pomoći u održavanju softvera ili računalnog komunikacijskog sustava).

13. O problemima u radu računalne opreme te eventualnim ugrozama iste, korisnik mora odmah obavijestiti administratora sustava.

14. Korisnici ne smiju samovoljno isključiti protuvirusnu zaštitu na svome računalu. Ako iz nekog razloga moraju privremeno zaustaviti protuvirusni program, korisnici moraju obavijestiti administratora sustava.

15. Korisnik će prekinuti korištenje aplikacija koje pristupaju poslovnim bazama podataka ako na računalu na kojem radi nije instaliran, ili se redovito ne ažurira program za zaštitu od virusa i drugog malicioznog softvera. O tome odmah mora obavijestiti dekana i čekati daljnje upute.

16. Nije dopuštena instalacija i kopiranje ili umnožavanje programske podrške bez odobrenja administratora sustava. Nije dopušteno korištenje programa ili elektroničkih dokumenata nad kojima postoji autorsko pravo ako korisnik ili Škola nema regulirano pravo njihovog korištenja.

17. Administrator sustava neće pružati informatičku podršku za aplikacije koje nisu nabavljene službenim putem u svrhu obavljanja poslovnih procesa Škole.

18. Prijenosna računala i drugu prijenosnu opremu koju rabi više korisnika, korisnici ne smiju iznositi izvan Škole bez odobrenja administratora sustava.

19. Korisnici se trebaju s pažnjom odnositi prema povjerenoj im računalnoj opremi.

20. Korisnik će se smatrati odgovornim za štete nastale na računalnoj opremi ako su nastale uslijed nepažnje ili nepravilne uporabe.

Uporaba Interneta i elektroničke pošte

Članak 12.

1. Korisnik treba voditi računa o pravilima ponašanja korisnika Interneta. Zabranjuje se pregledavanje mrežnih stranica s neprihvatljivim sadržajima.

2. Korisnici informacijskih sustava Škole u svrhu službene komunikacije obvezno moraju koristiti službeno im dodijeljenu adresu elektroničke pošte.

3. Korisnik za pristup elektroničkoj pošti smije upotrijebiti samo svoje osobno korisničko ime. Pojedini korisnici mogu biti ovlašteni za pristup grupnim adresama elektroničke pošte (primanje, ili primanje i slanje elektroničke pošte).

4. Korisnik elektroničke pošte odgovoran je za sve aktivnosti nastale s njegove adrese elektroničke pošte, kao i za aktivnosti nastale tijekom njegovog pristupa elektroničkoj pošti namijenjenoj posebnim aktivnostima Škole. Korisnik nikada i nikome ne smije otkrivati korisničko ime i lozinku za pristup računalnoj opremi, jer se mogu iskoristiti za pristup korisnikovom sustavu elektroničke pošte. Ako korisnik smatra da mu je lozinka ugrožena (poznata drugim osobama), obvezan ju je promijeniti.

5. Škola je vlasnik sve elektroničke pošte koja se šalje i prima pomoću računa elektroničke pošte koje je dodijelila Škola. Dekan od korisnika uvijek može zatražiti uvid u elektroničku poštu koja se nalazi na tim računima. U slučaju zloupotrebe elektroničke pošte, Dekan može zatražiti zatvaranje računa elektroničke pošte koju koristi zaposlenik Škole.

6. Korisnik sustava elektroničke pošte ne smije slati poruke elektroničkom poštom ljudima koje ne poznaje, ako oni sami to od korisnika nisu zatražili ili ako to nije sastavni dio radnih zadataka koje obavlja.

7. Neke adrese elektroničke pošte mogu predstavljati grupu ljudi, pa korisnik sustava elektroničke pošte to treba imati u vidu glede sadržaja poruke koju šalje.

8. U poruci elektroničke pošte korisnik se uvijek treba predstaviti svojim imenom i prezimenom, nazivom radnog mjesta, ali i nazivom i adresom sjedišta Škole.

9. Svi korisnici ispod svog potpisa u porukama elektroničke pošte trebaju obavezno navesti sljedeći tekst odricanja od odgovornosti: ''Ova elektronička poruka i njeni prilozi mogu sadržavati…''.

10. Korisniku sustava elektroničke pošte zabranjeno je:

- slanje komercijalnih oglasa (spam mail)
- slanje veće količine nezatraženih poruka (koje nisu rezultat radnih zadataka koje korisnik obavlja) na istu adresu elektroničke pošte, slanje poruka kojim se zahtijeva ili sudjeluje u tzv. lancima sreće

- lažno predstavljanje u sustavu elektroničke pošte
- krivotvorenje zaglavlja poruke elektroničke pošte
- uznemiravanje putem poruka elektroničke pošte u bilo kojem obliku
- činiti radnje koje predstavljaju kršenje pozitivnih domaćih i međunarodnih propisa.

11. Pri slanju privitaka korisnik treba biti siguran da primatelj na svome računalu ima odgovarajuće aplikacije kojima te dokumente može pregledati. Pri slanju privitaka pošiljatelj je dužan voditi računa da ne krši autorska prava ili poslovnu tajnu.

12. Ako se osobni podaci za službenu uporabu šalju elektroničkom poštom, na vrhu elektroničke poruke obvezno treba staviti napomenu kako se radi o podacima za službenu upotrebu.

13. Korisnik ne smije slati elektroničkom poštom nezaštićene osjetljive i povjerljive podatke (poput osobnih podataka, dijelova poslovnih baza podataka, PIN-a kartice ili lozinke za pristup računalnom sustavu itd.), zato što je standardna elektronička poruka nezaštićen medij za prijenos informacija i podataka.

14. Korisnik nikada ne smije otvarati privitak ili odabirati poveznicu (link) ako nije siguran da su oni namijenjeni njemu ili ako ima sumnju u vjerodostojnost adrese elektroničke pošte s koje mu je poruka upućena. Takve poruke elektroničke pošte može proslijediti administratoru sustava radi upute što dalje treba učiniti sa sumnjivom porukom.

15. Obvezno je periodično brisanje ili arhiviranje elektroničke pošte (kako iz mape Ulazna pošta, tako i iz mapa Poslano i Obrisano). Ovakvim postupanjem izbjegavaju se upozorenja o prekoračenom limitu prostora za pohranu elektroničkih poruka i omogućuje se nesmetan rad poslužitelja elektroničke pošte.

16. Administratori poslužitelja elektroničke pošte dužni su konfigurirati računala na taj način da se što više neželjenih poruka zaustavi i preusmjeri u mapu neželjenih poruka.

17. Korisnicima treba omogućiti da samostalno odrede koje su poruke prema njihovom mišljenju za njih spam.

Pohranjivanje podataka

Članak 13.

Radi odgovarajuće zaštite podatka kod pohranjivanja podataka potrebno je pridržavati se sljedećih uputa:

1. Mediji s podacima i programskom podrškom (CD diskovi, USB stick, eksterni HDD i ostali mediji) za vrijeme kada nisu u upotrebi ne smiju biti izloženi na lako dostupnim mjestima te se treba osigurati da ne budu dostupni neovlaštenim osobama.

2. Mediji koji sadrže povjerljive i važne podatke trebaju biti pohranjeni u adekvatnim zaključanim kasama ili metalnim ormarima.

3. Podatkovni mediji trebaju se zaštititi od nepovoljnih utjecaja okoline kao što su toplina, direktno sunčevo svjetlo, vlaga, elektromagnetska polja i slično.

4. Administrator sustava zadužen je za pohranu sigurnosnih kopija podataka (backup) koji se nalaze na računalnoj infrastrukturi Škole.

5. Za podatke koje korisnik pohrani na svom računalu odgovoran je korisnik. Ustanova ne snosi nikakvu odgovornost za podatke koji su spremljeni na lokalnim diskovima korisnika.

Intelektualno vlasništvo i licenčna prava

Članak 14.

Ustanova za obavljanje djelatnosti koristi isključivo licencirane računalne programe i aplikacije sukladno pozitivnim propisima o zaštiti intelektualnog vlasništva.

Na računalima i mobilnim uređajima u vlasništvu Škole ne smije se bez odobrenja administratora sustava koristiti programska podrška nabavljena privatno, bilo kupnjom ili donacijom. Legalnost licenci donirane programske podrške utvrđuje se Ugovorom o donaciji.

Članak 15.

Administrator sustava obvezan je:

- održavati ažuran popis programskih licenci u vlasništvu Škole
- čuvati licenčne ugovore ili uvjete korištenja programske potpore
- periodički, metodom slučajnog odabira, pregledati računala u vlasništvu Škole radi provjere uporabe samo legalne programske podrške.

Članak 16.

Korisnicima se zabranjuje:

- koristiti programsku podršku na način koji nije u skladu s licenčnim pravima proizvođača
- instalirati aplikacije koje nije odobrio administrator sustava na računala u vlasništvu Škole

- na računala u vlasništvu Škole instalirati programsku podršku koja nije licencirana ili nije u vlasništvu Škole
- kopirati programsku podršku bez prethodnog odobrenja administratora sustava

- preuzimati programsku podršku s Interneta bez prethodnog odobrenja administratora sustava.

Mjere sigurnosti

Članak 17.

Škola štiti svoju računalnu opremu, sklopovlje, programsku podršku, podatke i dokumentaciju od zlouporabe, krađe, neovlaštene uporabe i utjecaja okoliša.

Računalna oprema koja obavlja kritične funkcije nužne za funkcioniranje informacijskog sustava Ustanove ili sadrži povjerljive osobne podatke, štiti se fizičkim, tehničkim i organizacijskim mjerama zaštite.

Prostor u kome se nalazi računalna oprema treba biti zaštićen od poplava, požara i slično te treba poduzeti raspoložive mjere da se oprema i podaci zaštite te da se osigura što brži oporavak.

U tijeku radnog vremena dokumenti i drugi izvori podataka, kao i sredstva automatske obrade dokumenata, ne smiju se ostavljati bez nadzora.

Nakon završetka radnog vremena zaposlenici su obvezni službene dokumente i druge izvore podataka, pečate, žigove i štambilje, prijenosne informatičke medije (USB, CD) držati zaključane u ladicama ili ormarima u radnim prostorima.

Članak 18.

Korisnici računalne i telekomunikacijske opreme dužni su s pažnjom i odgovornošću brinuti o raspoloživoj opremi, bez obzira na to tko je njezin vlasnik, čuvajući je od oštećivanja i otuđenja.

Administrator sustava odgovoran je za održavanje ažurnim popisa sve računalne opreme, s popisom ugrađenih glavnih modula komponenti, inventarskim brojevima itd.

Za fizičku sigurnost opreme odgovoran je dekan. Ona odgovornost za pojedine uređaje može prenijeti na druge zaposlenike, koji potpisuju dokument kojim potvrđuju da su preuzeli ispravnu i sigurnu opremu.

Neprekidnost poslovanja

Članak 19.

Neprekidnost poslovanja obuhvaća uspostavljanje i testiranje adekvatne procedure sigurnosne pohrane podataka radi vraćanja sustava i podataka u prvobitno stanje nakon incidenta (pad sustava, prirodne nepogode, djelovanje računalnih virusa i dr.).

Planiranjem djelovanja u izvanrednim okolnostima utvrđuju se i analiziraju potencijalni problemi pri radu sustava i definiraju se postupci za rješavanje tih problema te definiraju druge metode korištenja, u slučaju nedostupnosti resursa informacijskog sustava, s ciljem održavanja kontinuiteta poslovanja.

Kako bi se sačuvali podaci u slučaju nezgoda poput kvarova na sklopovlju, požara, ili ljudskih grešaka, potrebno je redovito izrađivati rezervne kopije svih vrijednih informacija, uključujući i konfiguraciju softvera.

Preporučuje se izrada više kopija koje se čuvaju na različitim mjestima, po mogućnosti u vatrootpornim ormarima.

Upravljanje povjerljivim podacima

Članak 20.

Upravljanje povjerljivim osobnim podacima regulirano je Pravilnikom o zaštiti osobnih podataka, koji zajedno s predmetnim Pravilnikom čine Politiku informacijske sigurnosti i zaštite osobnih podataka.

Rješavanje sigurnosnih incidenata

Članak 21.

Svaki zaposlenik, student, suradnik te drugi korisnik informacijskog sustava Škole dužan je prijavljivati sigurnosne incidente, poput usporenog rada sustava, nemogućnosti pristupa, gubitka ili neovlaštene izmjene podataka, pojave virusa itd.

Administrator sustava zaprima obavijesti u slučaja incidenata, prikuplja potrebne informacije i izvještava dekana. Incidente treba dokumentirati kako bi se pomoglo u nastojanju da se izbjegnu slične situacije u budućnosti.

Postupanje u vezi sa sigurnosnim incidentima regulirano je posebnom internom uputom koja regulira proceduru u slučaju sigurnosnih incidenata.

Svrha predmetne procedure je utvrđivanje obveze prijavljivanja sigurnosnih incidenata te razrada mjera i postupaka radi istrage i rješavanja sigurnosnih incidenata.

Dekan odobrava istragu u vezi sa sigurnosnim incidentima te prema potrebi obavještava nadležna tijela.

Završne odredbe

Članak 22.

Svi korisnici informacijskog sustava Škole dužni su pridržavati se odredbi ovog Pravilnika, pridruženih procedura i uputa, kao i svih drugih internih odluka koje reguliraju korištenje informacijskog sustava i računalne opreme.

Kršenje odredbi ovog Pravilnika predstavlja povredu radne discipline i može korisnika izložiti opozivu prava uporabe informacijskog sustava Škole te pokretanju stegovnog postupka sve do prestanka ugovora o radu iz razloga uvjetovanog iskrivljenim ponašanjem radnika ili prestanka drugih primjenjivih ugovora.

Članak 23.

Dekan je dužan svakog novog korisnika informacijskih sustava Škole, prije nego li mu se odobri korisnički račun, upoznati sa sadržajem ovog Pravilnika.

Nakon upoznavanja s odredbama ovog Pravilnika korisnik potpisuje Izjavu o povjerljivosti, čime potvrđuje da je upoznat s mjerama sigurnosti informacijskog sustava i zaštite osobnih podataka.

Potpisana Izjava pohranit će se u dosje korisnika.

Članak 24.

Ovaj Pravilnik stupa na snagu danom donošenja i bit će objavljen na oglasnoj ploči i internim mrežnim stranicama Škole.

U Zagrebu, 13.5.2018.

Klasa: 602-04/18-01/01

Ur. broj: 251-376-01-18-20

Dekan:

dr.sc. Nenad Kacian

Upravno vijeće Visoke škole za sigurnost prihvatilo je ovaj pravilnik na sjednici: 8.6.2018.

Predsjednica Upravnog vijeća:

prof.dr.sc. Jadranka Mustajbegović

Pravilnik je objavljen na internetskoj stranici Visoke škole za sigurnost: 13.5.2018.