VISOKA TEHNIČKA ŠKOLA STRUKOVNIH STUDIJA – SUBOTICA
SZABADKAI MŰSZAKI SZAKFŐISKOLA – SZABADKA
SUBOTICA TECH – COLLEGE OF APPLIED SCIENCES
MARKA OREŠKOVIĆA 16, 24000 SUBOTICA, SERBIA
www.vts.su.ac.rs
Tel: +381 (0)24/655-201
Fax: +381 (0)24/655-255
email: office@vts.su.ac.rs

Datum: 05.06.2017.
Br.: 01-202/2017

PREDMET: BEZBEDNOSNA POLITIKA UNUTAR IKT SISTEMA ŠKOLE

Na osnovu člana 16. Statuta Visoke tehničke škole strukovnih studija u Subotici, na sednici Saveta koja je održana dana 05.06.2017. godine, usvojena je

BEZBEDNOSNA POLITIKA UNUTAR IKT SISTEMA ŠKOLE

Pojedini termini u ovom dokumentu imaju sledeće značenje:

1) informaciono-komunikacioni sistem (IKT sistem) je tehnološko-organizaciona celina koja obuhvata:
   (1) elektronske komunikacione mreže u smislu Zakona koji uređuje elektronske komunikacije;
   (2) uređaje ili grupe međusobno povezanih uređaja, takvih da se u okviru uređaja, odnosno u okviru barem jednog iz grupe uređaja, vrši automatska obrada podataka korišćenjem računarskog programa;
   (3) podatke koji se pohranjuju, obrađuju, pretražuju ili prenose pomoću sredstava iz podtač. (1) i (2) ove tačke, a u svrhu njihovog rada, upotrebe, zaštite ili održavanja;
   (4) organizacionu strukturu putem koje se upravlja IKT sistemom;
2) operator IKT sistema je zaposleni Škole imenovan odlukom Direktora Škole;
3) informaciona bezbednost predstavlja skup mera koje omogućavaju da podaci kojima se rukuje putem IKT sistema budu zaštićeni od neovlašćenog pristupa, kao i da se zaštiti integritet, raspoloživost, autentičnost i neporecivost tih podataka, da bi taj sistem funkcionisao kako je predviđeno;
4) tajnost je svojstvo koje znači da podatak nije dostupan neovlašćenim licima;
5) integritet znači očuvanost izvornog sadržaja i kompletnosti podatka;
6) raspoloživost je svojstvo koje znači da je podatak dostupan i upotrebljiv na zahtev ovlašćenih lica onda kada im je potreban;
7) autentičnost je svojstvo koje znači da je moguće proveriti i potvrditi da je podatak stvorio ili poslao onaj za koga je deklarisano da je tu radnju izvršio;
8) neporecivost predstavlja sposobnost dokazivanja da se dogodila određena radnja ili da je nastupio određeni događaj, tako da ga naknadno nije moguće poreći;
9) rizik znači mogućnost narušavanja informacione bezbednosti, odnosno mogućnost narušavanja tajnosti, integriteta, raspoloživosti, autentičnosti ili neporecivosti podataka ili narušavanja ispravnog funkcionisanja IKT sistema;

10) upravljanje rizikom je sistematičan skup mera koji uključuje planiranje, organizovanje i usmeravanje aktivnosti kako bi se obezbedilo da rizici ostanu u propisanim i prihvatljivim okvirima;
11) incident je unutrašnja ili spoljna okolnost ili događaj kojim se ugrožava ili narušava informaciona bezbednost;
12) mere zaštite IKT sistema su tehničke i organizacione mere za upravljanje bezbednosnim rizicima IKT sistema;
13) tajni podatak je podatak koji je, u skladu sa propisima o tajnosti podataka, određen i označen određenim stepenom tajnosti;
14) IKT sistem za rad sa tajnim podacima je IKT sistem koji je u skladu sa zakonom određen za rad sa tajnim podacima;
15) organ javne vlasti je državni organ, organ autonomne pokrajine, organ jedinice lokalne samouprave, organizacija kojoj je povereno vršenje javnih ovlašćenja, pravno lice koje osniva Republika Srbija, autonomna pokrajina ili jedinica lokalne samouprave, kao i pravno lice koje se pretežno, odnosno u celini finansira iz budžeta;
16) služba bezbednosti je služba bezbednosti u smislu zakona kojim se uređuju osnove bezbednosno-obaveštajnog sistema Republike Srbije;
17) kompromitujuće elektromagnetno zračenje (KEMZ) predstavlja nenamerne elektromagnetne emisije prilikom prenosa, obrade ili čuvanja podataka, čijim prijemom i analizom se može otkriti sadržaj tih podataka;
18) bezbednosna zona je prostor ili prostorija u kojoj se, u skladu sa propisima o tajnosti podataka, obrađuju i čuvaju tajni podaci;
19) informaciona dobra obuhvataju podatke u datotekama i bazama podataka, programski kod, konfiguraciju hardverskih komponenata, tehničku i korisničku dokumentaciju, unutrašnje opšte akte, procedure i slično.

BEZBEDNOSNA POLITIKA

Stav ovog akta je da sistem informacione bezbednosti ne može potpuno eliminisati ugroženost. Uvek treba da se teži u pravcu smanjenja rizika, što znači da faktore rizika uvek treba držati pod kontrolom.
Upravljanje bezbednosnim sistemom obuhvata: preventivne zadatke radi sprečavanja incidenta, radnje kontinualnog nadzora radi blagovremene detekcije incidenta i radnje brze i efikasne reakcije radi minimizacije štete.

Prilikom planiranja i primene mera zaštite IKT sistema treba se rukovoditi načelima:
1) načelo upravljanja rizikom - izbor i nivo primene mera se zasniva na proceni rizika, potrebi za prevencijom rizika i otklanjanja posledica rizika koji se ostvario, uključujući sve vrste vanrednih okolnosti;
2) načelo sveobuhvatne zaštite - mere se primenjuju na svim organizacionim, fizičkim i tehničko-tehnološkim nivoima, kao i tokom celokupnog životnog ciklusa IKT sistema;
3) načelo stručnosti i dobre prakse - mere se primenjuju u skladu sa stručnim i naučnim saznanjima i iskustvima u oblasti informacione bezbednosti;

4) načelo svesti i osposobljenosti - sva lica koja svojim postupcima efektivno ili potencijalno utiču na informacionu bezbednost treba da budu svesna rizika i poseduju odgovarajuća znanja i veštine.

Po načelu sveobuhvatnosti kod IKT sistema Škole treba uzeti u obzir sledeće element:
Energetika; Fizička zaštita; Zaštita od požara; Klimatizacija; Pravljenje sigurnosnih kopija; Definisanje klase zaštite: visoki prioritet, srednji prioritet, niski prioritet.
Definisanje dela sistema sa najvećim rizikom.

Predsednik Saveta

Dr Pinter Robert