UVAJANJE INFORMACIJSKE VARNOSTNE POLITIKE NA UNIVERZI V MARIBORU

Informacijska varnost obsega varovanje in zaščito vseh kritičnih, poslovno občutljivih, tajnih, osebnih in drugače občutljivih podatkov ter informacijsko telekomunikacijske tehnologije (ITkT) oziroma sisteme, ki so namenjeni obdelavi (oblikovanju, shranjevanju, spreminjanju, analiziranju, itd.) teh podatkov.

Prvenstveni motiv uvajanja informacijske varnostne politike je bila sicer ureditev stanja na UM na področju informacijske varnosti, vendar smo pri pripravi sledili tudi cilju pozitivnega vplivanja na ravnanje uporabnikov v smislu zavedanja (ne)varnosti uporabe ITkT. Predviden dolgoročni cilj UM je tudi certifikacija po standardu družine ISO 2700X in kasneje tudi po standardu BS 25599.

Predlagana informacijska varnostna politika, ki je s strani prorektorja za informatiko prof. dr. Tomaža Kerna, po predhodni potrditvi kolegija rektorja, predložena v proceduro sprejemanja na Univerzi v Mariboru in bo po končani proceduri posredovana senatu UM v potrditev, je sklop štirih dokumentov v skupnem obsegu 59 strani:

- krovna varnostna politika
- dokument, ki podrobneje opisuje varnost na področju ITkT
- varnostna politika za uporabnike
- varnostna politika za zunanje izvajalce

NAMEN varnostne politike je:

- definirati takšno ravnanje zaposlenih in drugih deležnikov, ki je z vidika informacijske varnosti sprejemljivo za Univerzo v Mariboru;
- objaviti širok konsenz glede varnostnih zahtev in prakse;
- zapisati pravno podlago za ukrepanje ob neustreznem ravnanju zaposlenih in drugih deležnikov;
- definirati zahteve za varnostna preverjanja in ukrepe;
- vodstvu in drugim deležnikom, vključno z revizorji, predstaviti indikatorje, ki omogočajo validiranje zrelosti informacijske varnosti in skladnosti s predpisi ter
- definirati pogoje, pod katerimi je dovoljena izmenjava informacij in dostop do poslovnih aplikacij.

CILJNA PUBLIKA so uporabniki ITkT storitev (zaposleni, študenti, zunanji sodelavci) ter zunanji izvajalci.

V dokumentih, ki so bili pripravljeni s pomočjo zunanjega podjetja, pregledani in dopolnjeni s strani strokovnega osebja (RCUM) ter visokošolskih učiteljev UM s področja informacijske varnosti, so upoštevane posebnosti javne univerze. Dokumenti so bili tudi predhodno predloženi osebam, odgovornim za informacijsko tehnologijo – dobljene pripombe so upoštevane. Pri pripravi dokumenta smo upoštevali obstoječo organiziranost UM, njeno organizacijsko kulturo in dosedanjo dobro prakso na tem področju. Dokumenti so bili pregledani tudi s strani informacijskega pooblaščenca.

Dokumenti IvP ne morejo rešiti vseh potencialnih težav na tem področju. Upoštevane so tiste, rešitve ki so lahko realistično implementirane ter upoštevane v naslednjem koledarskem letu

in hkrati odpravljajo največja tveganja in nejasnosti. Načrtovano je, da se revizija dokumentov opravi vsako leto po sprejemu tega dokumenta.

Na nivoju UM trenutno ni zaposlenega človeka, ki bi pokrival to področje (skrbnik informacijske varnosti, tudi informacijski varnostni inženir (angl. chief information security officer - CISO)). Le-ta ima celotno odgovornost za razvoj in vpeljavo sistema vodenja varovanja informacij. Senatu UM se zato predlaga, da se hkrati s sprejemom tega dokumenta zagotovijo finančna sredstva za zapolnitev delovnega mesta v okviru RCUM s 1. 1. 2013 (priloga: opis delovnega mesta skrbnika informacijske varnosti).

Uporabljeni dodatni viri:

Gartner, Roundup of Security and IT Risk Management Policy Guidance and Templates, 2Q12, 2012

Gartner, Planning Information Security and Risk Management Policy, 2012

Hajtnik Tatjana, Priporočila za pripravo informacijske varnostne politike, Center Vlade RS za informatiko, 2002

Maribor, 18. 6. 2013

Pripravil: dr. Izidor Golob, pomočnik glavne tajnice

Predlagatelj: prof. dr. Tomaž Kern, prorektor

DOKUMENTI, KI SO PREDLOŽENI SENATU V SPREJEM:

- Krovna informacijska varnostna politika
- Informacijska varnostna politika za področje IT
- Informacijska varnostna politika za uporabnike
- Informacijska varnostna politika za zunanje izvajalce

PRILOGA: OPIS DELOVNEGA MESTA ZA SKRBNIKA INFORMACIJSKE VARNOSTI

- priprava in vzdrževanje dokumentov varnostne politike
- razvoj postopkov za zagotavljanje splošne integritete omrežja in sistemov
- izvajanje analiz in obravnavanje tveganj
- zagotavljanje ozaveščenosti zaposlenih glede varovanja informacij ter ustrezne usposobljenosti upravljanja z varnostnimi incidenti
- izvajanje varnostnih ukrepov za izboljšanje stanja varovanja informacij
- izvajanje nalog na področju projektiranja, varovanja in izkoriščanja informacijske infrastrukture
- načrtovanje preventivnih ukrepov
- pripravljanje predlogov in izvedba korektivnih ukrepov ob varnostnih incidentih