PRAVILNIK O INFORMACIJSKOJ SIGURNOSTI VELEUČILIŠTA VELIKA GORICA

VELIKA GORICA, 2023

Na temelju članka 20. stavka 3. Statuta Veleučilišta Velika Gorica od 17. ožujka 2023. godine, KLASA: 602-03/23-14/005, URBROJ: 238/31-132-056-23-01 dekan Veleučilišta Velika Gorica donosi

PRAVILNIK O INFORMACIJSKOJ SIGURNOSTI VELEUČILIŠTA VELIKA GORICA

I. OPĆE ODREDBE

Članak 1.

(1) Informacije koje se prikupljaju, analiziraju, pohranjuju, komuniciraju i o njima izvještavaju mogu biti predmet krađe, zlouporabe, gubitka i korupcije. Informacije mogu biti dovedene u opasnost zbog lošeg obrazovanja i obuke te kršenja sigurnosnih kontrola. Sigurnosni incidenti mogu dovesti do neugodnosti, financijskih gubitaka, nepoštivanja standarda i zakona, kao i mogućih presuda protiv Veleučilišta Velika Gorica (u daljnjem tekstu: Veleučilište).

(2) Ovaj Pravilnik o informacijskoj sigurnosti (u daljnjem tekstu: Pravilnik) stoji uz Proceduru o informacijskoj sigurnosti Veleučilišta te Pravilnikom o obradi i zaštiti osobnih podataka kako bi pružio nacrt za upravljanje informacijskom sigurnošću na visokoj razini i opravdanje za kontrole sigurnosti informacija Veleučilišta koje se temelje na riziku.

II. CILJEVI

Članak 2.

(1) Sigurnosni ciljevi Veleučilišta su:

a. Ovlašteni korisnici Veleučilišta mogu sigurno pristupiti i dijeliti informacije kako bi obavljali svoje uloge
b. Informacijski rizici Veleučilišta su identificirani, upravljani i tretirani u skladu s dogovorenom tolerancijom rizika
c. Fizičke, proceduralne i tehničke kontrole Veleučilišta balansiraju korisničko iskustvo i sigurnost
d. Nastavna, istraživačka i administrativna djelatnost Veleučilišta uzima u obzir informacijsku sigurnost
e. Pojedinci koji pristupaju informacijama Veleučilišta svjesni su svojih odgovornosti za informacijsku sigurnost
f. Incidenti koji utječu na informacijsku imovinu Veleučilišta se rješavaju i iz njih se uči kako bi se poboljšale kontrole Veleučilišta
g. Veleučilište ispunjava ugovorne i zakonske obveze koje se odnose na informacijsku sigurnost

III. DJELOKRUG

Članak 3.

(1) Pravilnik informacijske sigurnosti i njegove prateće procedure, politike i procesi primjenjuju se na sve informacije koje se koriste na Veleučilištu, u svim formatima. To uključuje informacije koje obrađuju druge organizacije u svom poslovanju sa Veleučilištem.
(2) Pravilnik informacijske sigurnosti i njegove prateće kontrole, procesi i procedure primjenjuju se na sve pojedince koji imaju pristup informacijama i tehnologijama Veleučilišta, uključujući vanjske strane koje Veleučilištu pružaju usluge obrade informacija.
(3) Detaljan opseg, uključujući raščlambu korisnika, informacijske imovine i sustava za obradu informacija, uključen je u Okvirni dokument sustava upravljanja sigurnošću informacija (ISMS).

IV. USKLAĐENOST

Članak 4.

(1) Usklađenost s kontrolama u ovom pravilniku nadzirati će tim za informacijsku sigurnost i izvještavati Povjerenstvo za informacijsku sigurnost Veleučilišta. Povjerenstvo za sigurnost informacijskog sustava formira Veleučilište s ciljem kvalitetnijeg sveukupnog upravljanja informacijskom sigurnošću Veleučilišta.
(2) Tim za informacijsku sigurnost sastoji se od upravitelja informacijskom sigurnošću (u daljnjem tekstu: ISMS voditelja) a kojeg određuje dekan Veleučilišta, te od članova informatičke podrške određene od strane ISMS voditelja.
(3) Čelnici ustrojbenih cjelina obvezni su u svojim ustrojbenim cjelinama osigurati da svi korisnici budu upoznati s ovim Pravilnikom, te da ga se pridržavaju.

V. PREGLED

Članak 5.

(1) ISMS voditelj provodit će pregled ove politike jednom godišnje ili češće prema potrebi, a odobriti će je Povjerenstvo za informacijsku sigurnost Veleučilišta i Stručno vijeće Veleučilišta.

VI. GLAVNE ODREDBE PRAVILNIKA

Članak 6.

(1) Politika Veleučilišta je osigurati da informacije budu zaštićene od gubitka:
   a. Povjerljivosti – informacije će biti dostupne samo ovlaštenim osobama
   b. Integriteta – održavat će se točnost i potpunost informacija
   c. Dostupnosti – informacije će biti dostupne ovlaštenim korisnicima i procesima po potrebi

(2) Veleučilište će implementirati Sustav upravljanja informacijskom sigurnošću temeljen na međunarodnom standardu za informacijsku sigurnost ISO 27001. Veleučilište će se također pozivati na druge standarde prema potrebi, kao što su NIST, vodeći računa o pristupima koje su usvojili njegovi dionici, uključujući istraživačke partnere.
(3) Veleučilište će usvojiti pristup koji se temelji na riziku u primjeni kontrola:
    1. Politika informacijske sigurnosti
    2. Organizacija informacijske sigurnosti
    3. Sigurnost ljudskih resursa
    4. Upravljanje imovinom
    5. Kontrola pristupa
    6. Kriptografija
    7. Fizička sigurnost i sigurnost okruženja
    8. Operativna sigurnost
    9. Sigurnost komunikacija
    10. Stjecanje, razvoj i održavanje sustava
    11. Odnosi s dobavljačima
    12. Upravljanje incidentima informacijske sigurnosti
    13. Upravljanje kontinuitetom poslovanja iz aspekta informacijske sigurnosti
    14. Usklađenost

VII. POLITIKA INFORMACIJSKE SIGURNOSTI

Članak 7.

(1) Definirati će se niz politika, procesa i procedura niže razine za informacijsku sigurnost, kao potpora Pravilniku informacijske sigurnosti visoke razine i njezinim navedenim ciljevima. Ovaj paket prateće dokumentacije odobrit će Povjerenstvo za informacijsku sigurnost Veleučilišta i Stručno vijeće Veleučilišta, objavit će ga i priopćiti korisnicima Veleučilišta i relevantnim vanjskim stranama.

VIII. ORGANIZACIJA INFORMACIJSKE SIGURNOSTI

Članak 8.

(1) Veleučilište će definirati i implementirati odgovarajuće upravljačke aranžmane za upravljanje informacijskom sigurnošću. To će uključivati identifikaciju i dodjelu sigurnosnih odgovornosti, za pokretanje i kontrolu provedbe i rada informacijske sigurnosti unutar Veleučilišta.
(2) Veleučilište će imenovati najmanje:
    a. Jednog izvršitelja koji predsjeda Povjerenstvom za informacijsku sigurnost i preuzima odgovornost za informacijski rizik, odnosno dekana Veleučilišta
    b. Povjerenstvo za informacijsku sigurnost koje utječe, nadzire i promiče učinkovito upravljanje informacijama Veleučilišta
    c. ISMS voditelja za upravljanje svakodnevnom informacijskom sigurnošću

IX. SIGURNOST LJUDSKIH RESURSA

Članak 9.

(1) Sigurnosne politike Veleučilišta i očekivanja za prihvatljivo korištenje bit će priopćeni svim korisnicima kako bi se osiguralo da razumiju svoje odgovornosti.
(2) Obrazovanje i obuka o informacijskoj sigurnosti bit će dostupni cijelom osoblju, a loše i neprimjereno ponašanje će se adresirati u skladu s razinom povrede sigurnosti informacijskih sustava i informacija.
(3) Gdje je to praktično, sigurnosne odgovornosti bit će uključene u opise radnih mjesta i planove osobnog razvoja.

X. UPRAVLJANJE IMOVINOM

Članak 10.

(1) Sva imovina (informacije, softver, oprema za elektroničku obradu informacija, servisne usluge i ljudi) biti će dokumentirana i evidentirana. Vlasnici, odnosno ustrojstveno odgovorni zaposlenici će biti identificirani za svu imovinu i oni će biti odgovorni za održavanje i zaštitu svoje imovine.
(2) Sva informacijska imovina bit će klasificirana prema svojim zakonskim zahtjevima, poslovnoj vrijednosti, kritičnosti i osjetljivosti, a klasifikacija će ukazati na odgovarajuće zahtjeve za rukovanje. Sva informacijska imovina imat će definiran raspored zadržavanja i odlaganja.

XI. KONTROLA PRISTUPA

Članak 11.

(1) Pristup svim informacijama biti će kontroliran i vođen poslovnim zahtjevima. Pristup će se odobriti ili će se dogovoriti za korisnike prema njihovoj ulozi i klasifikaciji informacija, samo do razine koja će im omogućiti obavljanje svojih dužnosti.
(2) Za pristup svim informacijskim sustavima i uslugama održavati će se formalni postupak registracije i odjave korisnika. To će uključivati obvezne metode provjere autentičnosti temeljene na osjetljivosti informacija kojima se pristupa i uključivati će razmatranje više čimbenika prema potrebi.
(3) Za korisnike s povišenim privilegijama biti će implementirane posebne kontrole kako bi se smanjio rizik od nemarne ili namjerne zlouporabe sustava. Podjela dužnosti će se provoditi, gdje je to praktično.

XII. KRIPTOGRAFIJA

Članak 12.

(1) Veleučilište će osigurati smjernice i alate kako bi se osigurala ispravna i učinkovita upotreba kriptografije za zaštitu povjerljivosti, autentičnosti i integriteta informacija i sustava.

XIII. FIZIČKA SIGURNOST I SIGURNOST OKRUŽENJA

Članak 13.

(1) Objekti za obradu informacija smješteni su u sigurnim područjima, fizički zaštićeni od neovlaštenog pristupa, oštećenja i smetnji definiranim sigurnosnim perimetrima.
(2) Uspostavit će se višeslojne unutarnje i vanjske sigurnosne kontrole kako bi se spriječio neovlašteni pristup i omogućila zaštita imovine, posebno one koja je kritična ili osjetljiva od prisilnog ili prikrivenog napada.

XIV. OPERATIVNA SIGURNOST

Članak 14.

(1) Veleučilište će osigurati ispravan i siguran rad sustava za obradu informacija.
(2) To će uključivati:
    a. Dokumentirane operativne procedure
    b. Korištenje formalnih promjena i upravljanje kapacitetima
    c. Kontrole protiv zlonamjernog softvera
    d. Definirana upotreba zapisivanja sigurnosnih događaja na sustavima i aplikacijama
    e. Upravljanje ranjivostima

XV. SIGURNOST KOMUNIKACIJA

Članak 15.

(1) Veleučilište će održavati kontrole mrežne sigurnosti kako bi osiguralo zaštitu informacija unutar svojih mreža, te će osigurati alate i smjernice za osiguranje sigurnog prijenosa informacija kako unutar svojih mreža tako i s vanjskim entitetima, u skladu sa zahtjevima klasifikacije i rukovanja povezanim s tim informacija.

XVI. STJECANJE, RAZVOJ I ODRŽAVANJE SUSTAVA

Članak 16.

(1) Zahtjevi informacijske sigurnosti biti će definirani tijekom razvoja poslovnih zahtjeva za nove informacijske sustave ili promjene postojećih informacijskih sustava.
(2) Kontrole za ublažavanje svih identificiranih rizika bit će provedene tamo gdje je to prikladno.
(3) Razvoj sustava bit će podložan kontroli promjena i odvajanju testnog, razvojnog i operativnog okruženja.

XVII. ODNOSI S DOBAVLJAČIMA

Članak 17.

(1) Zahtjevi za informacijsku sigurnost Veleučilišta uzet će se u obzir prilikom uspostavljanja odnosa s dobavljačima, kako bi se osigurala zaštita imovine koja je dostupna dobavljačima.
(2) Aktivnosti dobavljača će se pratiti i revidirati prema vrijednosti imovine i povezanim rizicima.

XVIII. UPRAVLJANJE INCIDENTIMA INFORMACIJSKE SIGURNOSTI

Članak 18.

(1) Biti će dostupne smjernice o tome što predstavlja incident informacijske sigurnosti i kako ga treba prijaviti.
(2) Stvarne ili sumnjive povrede informacijske sigurnosti moraju se prijaviti i istražiti se.
(3) Poduzeti će se odgovarajuće korektivne radnje i svako učenje će biti ugrađeno u kontrole.

XIX. UPRAVLJANJE KONTINUITETOM POSLOVANJA IZ ASPEKTA INFORMACIJSKE SIGURNOSTI

Članak 19.

(1) Veleučilište će imati uspostavljene aranžmane za zaštitu kritičnih poslovnih procesa od posljedica velikih kvarova informacijskih sustava ili katastrofa te za osiguranje njihovog pravovremenog oporavka u skladu s dokumentiranim poslovnim potrebama.
(2) To će uključivati odgovarajuće rutine sigurnosnog kopiranja i ugrađenu otpornost.
(3) Planovi kontinuiteta poslovanja moraju se održavati i testirati kao podrška ovoj politici.
(4) Provesti će se analiza utjecaja na poslovanje od posljedica katastrofa, sigurnosnih kvarova, gubitka usluge i nedostatka dostupnosti usluga.

XX. USKLAĐENOST

Članak 20.

(1) Dizajn, rad, korištenje i upravljanje informacijskim sustavima moraju biti u skladu sa svim zakonskim, regulatornim i ugovornim sigurnosnim zahtjevima. Trenutačno to uključuje zakone o zaštiti podataka i ugovorne obveze Veleučilišta.
(2) Veleučilište će koristiti kombinaciju interne i po potrebi vanjske revizije kako bi pokazalo usklađenost s odabranim standardima i najboljom praksom, uključujući interne politike i procedure.
(3) To će uključivati provjere zdravlja IT sustava, analize nedostataka u odnosu na dokumentirane standarde, interne provjere usklađenosti osoblja i povrate od vlasnika informacijske imovine.

XXI. PRILOZI PRAVILNIKU

Članak 21.

(1) Procedure kontrole sigurnosti informacija opisuju kako će Veleučilište informacije čuvati sigurnima.

(2) Sljedeće procedure, pravilnici i politike izravno podržavaju Pravilnik informacijske sigurnosti te su sastavni dio ovog pravilnika kao priloženi dokumenti:

1. Politika prihvatljive uporabe informacijskih sustava Veleučilišta Velika Gorica
2. Procedura kontrole pristupa
3. Politika čistog stola i ekrana
4. Procedura kontrole računalstva u oblaku
5. Procedura sigurnosti komunikacija
6. Procedura kontrole usklađenosti
7. Procedura kontrole kriptografije
8. Procedura uništavanja podataka
9. Procedura upravljanja incidentima informacijske sigurnosti
10. Procedura o klasifikaciji informacija
11. Procedura upravljanja dnevnika sustava i forenzičke spremnosti
12. Procedure kontrole mobilnog i daljinskog pristupa
13. Procedure upravljanja lozinkama
14. Procedura provjere prije zapošljavanja
15. Procedura kontrole informacijske sigurnosti projekata
16. Procedura procjene rizika informacijske sigurnosti
17. Studentski pravilnik za korištenje računalnih resursa Veleučilišta Velika Gorica
18. Procedura odnosa s dobavljačima u kontekstu informacijske sigurnosti
19. Procedura upravljanja prijetnjama i ranjivostima
20. Procedura obuke i podizanja svijesti korisnika o informacijskoj sigurnosti
21. Politika kriznog planiranja za informacijske sustave

XXII. STUPANJE NA SNAGU PRAVILNIKA

Članak 22.

(1) Ovaj Pravilnik stupa na snagu danom donošenja.

KLASA: 602-03/23-14/039
URBROJ: 238/31-132-054-23-01
Velika Gorica, 07.12.2023.

VELEUČILIŠTE VELIKA GORICA 1 MMIII

Dekan

dr.sc. Ivan Toth, prof. v. š.