Osrednje območne knjižnice

mariborska knjižnica
Mariborska knjižnica, Rotovški trg 2, 2000 Maribor
tel.: +386 2 23 52 100, fax: +386 2 23 52 127, www.knjiznica-mb.si, info@mb.sik.si

Krovna informacijska varnostna politika splošne knjižnice

Vir: https://inbound.usisecurity.com/hs-fs/hubfs/Depositphotos_36515569_l-2015-min.jpg?width=620&name=Depositphotos_36515569_l-2015-min.jpg

Maribor, december 2023
dopolnitev december 2024

Krovna informacijska varnostna politika splošne knjižnice

Besedilo: **Irena Sirk** in **Anka Rogina,** Mariborska knjižnica

Ta dokument je nastal kot rezultat izvajanja kompetenčnih vsebin, v okviru delovanja Mariborske knjižnice kot osrednje območne knjižnice. Nastanek dokumenta je finančno podprlo Ministrstvo za kulturo RS.

Maribor, december 2023; dopolnitev, december 2024

Krovna informacijska varnostna politika splošne knjižnice

Uvod

Za uspešno poslovanje knjižnice so varne in zanesljive informacije in informacijska sredstva ključnega pomena. V ta namen knjižnica vodi sistem varovanja informacij, ki s svojimi politikami, pripadajočimi organizacijskimi predpisi in delovnimi navodili določa, kako informacije in informacijska sredstva zaščititi. S krovno informacijsko varnostno politiko vodstvo knjižnice izraža svojo odgovornost in zavezanost za zagotavljanje ustrezne varnosti informacij in informacijskih sredstev, zaposleni, pogodbeni partnerji in vsi uporabniki informacij in informacijskega sistema pa svojo odgovornost glede izvajanja informacijske varnostne politike knjižnice.
Z dokumentom se izraža in vzpostavlja odnos med informacijskim okoljem in uporabo njegovih sredstev na različnih nivojih. Informacijska varnostna politika je namenjena zaščiti podatkov, ki se združujejo v informacije za različne namene. Informacijska varnostna politika mora biti aktualna, zagotavljati mora celostno ureditev informacijskega sistema in uskladitev notranjih in zunanjih deležnikov, ki vstopajo in delujejo v informacijskem sistemu z različnimi standardi in zakonodajo s tega področja. Pravila delovanja in dolžnosti uporabnikov ter vzdrževalcev informacijskega sistema so namenjena preprečevanju morebitne škode ob najrazličnejših vdorih, kar je osnovni namen krovne informacijske varnostne politike. Predstavlja tudi uravnoteženje investicij v kibernetsko varnost z upoštevanjem ravnanj, ki jih varnostna politika predvideva. Informacijska varnostna politika mora biti skladna z rastjo in spremembami informacijskega sistema, ki ga obvladuje.
Informacijska varnost zajema postopke in metodologije, ki se izvajajo za zaščito zaupnih, zasebnih in občutljivih informacij ali podatkov v tiskani, elektronski ali kateri koli drugi obliki pred nepooblaščenim dostopom, uporabo, zlorabo, razkritjem, uničenjem ali spreminjanjem. Kibernetska varnost je podmnožica informacijske varnosti, osredotočena na varovanje digitalnih informacij in sredstev, kot so računalniški sistemi, omrežja in podatki, pred digitalnimi napadi. Informacijska varnost poleg kibernetske varnosti obravnava še organizacijo dela, fizično varovanje in spoštovanje standardov.

Krovna informacijska varnostna politika knjižnice predstavlja na enem mestu opisane cilje in obseg informacijske varnostne politike za zagotavljanje in upravljanje z informacijsko varnostjo za vse uporabnike informacijskega sistema. Določa varnostne vidike v skladu z varnostno občutljivostjo, poslovno vrednostjo in kritičnostjo informacij ne gleda na obliko, v kateri se informacije pojavljajo: na računalnikih, na papirju ali na prenosnih pomnilniških medijih ter pri prenosu preko omrežja oziroma pri ustnem posredovanju.
Krovna informacijska varnostna politika v podrednem dokumentu na 2. nivoju natančneje opredeljuje organizacijo upravljanja informacijske varnosti po področjih. Na 3. nivoju so navodila, postopki in obrazci, namenjeni za izvajanje varnostne politike knjižnice v praksi.

Slika 1: Struktura informacijske varnostne politike

Namen informacijske varnostne politike

Namen informacijske varnostne politike je zaščita informacij in informacijskih sredstev knjižnice pred vsemi nevarnostmi, notranjimi ali zunanjimi, namernimi ali nenamernimi. Namenjena je zagotavljanju treh najbolj pomembnih lastnosti informacij: zaupnosti, celovitosti in razpoložljivosti[1].

- **Zaupnost** pomeni zaščito občutljivih informacij pred nepooblaščenim dostopom ali protipravnim prestrezanjem. Zaupnost zagotavlja, da je informacija dostopna samo tistim, ki imajo ustrezna pooblastila. V primeru izpada drugih varnostnih mehanizmov (npr. ukraden prenosni računalnik, ukradeni podatki s strežnika) zaupnost zagotavlja, da so vsi podatki neuporabni - zapisani v nerazumljivi oz. neuporabni obliki.
- **Celovitost** obravnava zagotavljanje pravilnosti ter celovitosti informacij in programske opreme. Kontrola celovitosti se uporablja za zaščito podatkov in sistemov pred nepooblaščeno spremembo. Celovitost olajša ugotavljanje sprememb ter preprečuje, da bi spremenjeno kopijo obravnavali kot original.
- **Razpoložljivost** zagotavlja, da so informacije in poslovno pomembne storitve, aplikacije in procesi na voljo pooblaščenim uporabnikom, ko jih ti potrebujejo.

Cilj informacijske varnostne politike

Cilj informacijske varnostne politike je zagotoviti nemoteno in varno poslovanje knjižnice ter preprečiti škodo oz. zmanjšati posledice varnostnih incidentov na najmanjšo možno mero pri informacijah in podatkih, procesih v informacijskem sistemu knjižnice, komponentah informacijskega sistema (strojna, programska in ostala oprema), lokacijah delovanja knjižnice, zaposlenih v knjižnici, partnerjih in uporabnikih.

V ta namen informacijska varnostna politika zagotavlja:

- povečanje varnosti informacijskega sistema in njegovih posameznih delov,
- določitev pristojnosti in odgovornosti s področja informacijske varnosti na posameznih delovnih področjih knjižnice,
- zagotavljanje delovanja tudi v primeru varnostnih incidentov,

[1] Povzeto iz Krovna informacijska varnostna politika. Univerza v Mariboru, 2013

- skladnost ukrepov s področja informacijske varnosti z zakonodajo, predpisi in ustreznimi standardi.

Obseg informacijske varnostne politike

Vsaka knjižnica mora sama določiti velikost svojega sistema upravljanja informacijske varnosti. Pri tem mora upoštevati zunanje in notranje dejavnike, ki vplivajo na varnost podatkov, informacij, informacijskih sredstev, postopkov in procesov. Prav tako mora upoštevati zunanje in notranje deležnike, ki delujejo v njenem informacijskem sistemu, njihove potrebe in zahteve. Oceniti mora tudi lastne sposobnosti za doseganje informacijske varnosti.

Standard ISO/IEC 27001:2022 prikazuje štiri vidike varovanja informacij in informacijskih sredstev, ki jih spremlja s pomočjo 93 varnostnih kontrol:

- Organizacijski vidik (37 kontrol)
- Nadzor ljudi (8 kontrol)
- Fizično varovanje (14 kontrol)
- Tehnični nadzor (34 kontrol)

Informacijska varnostna politika zajema vse štiri navedene vidike varovanja in predvideva ustrezne ukrepe za doseganje želenih ciljev v okviru svojega sistema upravljanja informacijske varnosti.

Za uspešno obvladovanje organizacije informacijske varnostne politike je smiselno, da se v okviru krovne varnostne politike oblikujejo posamezne varnostne politike za prepoznane vidike varovanja (po standardu ISO/IEC 27001:2022).

Organizacijski varnostni vidik

Pomemben vidik informacijske varnosti je varovanje povezano z delovanjem in obnašanjem ljudi, ki ustvarjajo, vzdržujejo in uporabljajo informacijski sistem. V tem segmentu je zato zajeta organizacija poslovanja na tem področju, pa tudi ozaveščanje, izobraževanje in usposabljanje vseh zaposlenih o informacijski varnosti. Za konkreten opis nalog, odgovornosti in zadolžitev knjižnica oblikuje dokument, ki mora vsebovati vsaj naslednje vsebine:

- Odgovornosti vodstva
  Vodstvo knjižnice je odgovorno za izvajanje varnostne politike v celoti, za vpeljavo sistema vodenja varovanja informacij, za spremljanje in nadziranje učinkovitosti varnostnih ukrepov in postopkov ter za zagotavljanje potrebnih finančnih in človeških virov. Vodstvo mora od zaposlenih in pogodbenih partnerjev zahtevati informacijsko varnostno ravnanje v skladu z vzpostavljenimi politikami in postopki knjižnice.
- Vloge in odgovornosti na področju informacijske varnosti
  Za vsako delovno mesto v knjižnici je treba opredeliti odgovornosti na področju informacijske varnosti. Za uresničevanje ciljev informacijske varnosti na svojem delovnem področju so odgovorni vsi zaposleni v knjižnici, zato morajo biti z informacijsko varnostno politiko seznanjeni in so jo dolžni spoštovati. Vsi, ki imajo dostop do knjižničnega informacijskega sistema, morajo izpolnjevati zahteve informacijske varnostne politike. Vodstvo knjižnice lahko določi odgovorno osebo za izvajanje informacijske varnostne politike v knjižnici. Odgovorna

oseba, ki koordinira delo z zunanjimi izvajalci, je zadolžena, da se tudi zunanji izvajalci seznanijo z varnostno politiko in upoštevajo njena določila ter to tudi pisno potrdijo.

- Zasebnost in zaščita osebno določljivih podatkov
  Pri vseh postopkih in procesih je treba zagotoviti zasebnost in zaščito osebno določljivih podatkov, kot to zahtevajo ustrezna zakonodaja in predpisi.
- Ozaveščenost, izobraževanje in usposabljanje o informacijski varnosti
  Vsi zaposleni se morajo seznaniti s pravili varne uporabe informacijske infrastrukture. Zagotoviti je treba redna izobraževanja o informacijski varnosti za vse zaposlene in jih ozaveščati o pomenu upoštevanja pravil varne rabe informacijskega sistema knjižnice.
  Vsi zaposleni v knjižnici in po potrebi tudi pogodbeni partnerji morajo biti seznanjeni z rednimi posodobitvami organizacijskih politik in postopkov, pomembnih za njihovo delovno mesto.
- Poročanje o informacijskih varnostnih dogodkih
  Zaposleni morajo vodstvu knjižnice (ali odgovorni osebi za informacijsko varnost, če obstaja) čim prej sporočiti opažene varnostne incidente kot so varnostne pomanjkljivosti, namerne in nenamerne varnostne kršitve, nepravilno ali sumljivo delovanje sistemov ali programske opreme, nedelovanje sistemov, viruse, napake, grožnje in ranljivosti sistemov in storitev, ipd.
- Skladnost s politikami, pravili in standardi informacijske varnosti
  Redno je treba spremljati razvoj in spremembe na področju informacijske varnosti. Prav tako je treba spremljati spremembe in upoštevati veljavno zakonodajo, predpise in standarde. Redno je treba preverjati skladnost informacijske varnostne politike knjižnice s postopki, procesi, specifičnimi politikami, pravili ipd. v sami knjižnici.

Vsebino dokumenta knjižnica prilagodi svojim razmeram, pri določanju potrebnih kontrol pa upošteva tudi kontrole po standardu ISO/IEC 27001:2022.

Fizični in tehnični nadzor

Za doseganje informacijske varnosti je treba zagotoviti fizično zaščito informacijskih sredstev, obvladovanje dostopov ter ustrezno ravnanje z opremo, na kateri tečejo procesi obdelave podatkov in oblikovanja informacij. Tehnično upravljanje z opremo, ki omogoča delovanje informacijskega sistema knjižnice, pravila dostopov do podatkov in informacij, varovanje informacij pred izgubo na nivoju celotne knjižnice, upravljanje s posebnimi dostopi in razvoj informacijskega sistema ter informacijske varnosti vsebuje dokument, ki ima vsaj naslednje vsebine:

- Območje fizičnega varovanja
  Določiti je treba prostore v knjižnici, ki jih je treba posebej fizično varovati (npr. zaklepati), da bi preprečili poškodovanje, uničenje oz. nepooblaščeni dostop do občutljivih ali ključnih podatkov, informacij ali sistemov za obdelavo informacij.
- Vzdrževanje opreme
  Skrbeti je treba za pravilno stalno vzdrževanje opreme in informacijskih sredstev, da je mogoče zagotavljati razpoložljivost, celovitost in zaupnost informacij.
- Upravljanje tehničnih ranljivosti sistema
  Pravočasno je treba pridobiti informacije o tehničnih ranljivostih informacijskih sistemov v uporabi, ovrednotiti izpostavljenost knjižnice takim ranljivostim ter sprejeti ustrezne ukrepe za preprečevanje tveganja.
- Beleženje dogodkov
  Zapisovati, hraniti, zaščititi in analizirati je treba dnevnike dogodkov, ki beležijo aktivnosti uporabnikov, izjeme, okvare in druge varnostne dogodke.

- Omejitev dostopa do informacij
  Določiti je treba, kdo lahko dostopa do katere ravni informacijskega sistema knjižnice (do informacij, do informacijskih sredstev in do posebnih (administrativnih) pravic) ter kako se ureja uporaba in dostop. Predpisati je treba postopek ukinitve dostopa do informacijskih virov, ko ga zaposleni ne potrebuje več. O tem je treba voditi evidence.
- Varnostno kopiranje informacij
  Določiti je treba politiko varnostnega kopiranja pomembnih poslovnih informacij. Varnostne kopije podatkov, programske opreme in sistemov je treba vzdrževati in redno preizkušati.
- Upravljanje sprememb
  Ob spremembah zakonodaje, pojavu novih groženj, novih varnostnih incidentov, spremembah organizacije, poslovnih procesov, naprav za obdelavo informacij ali tehnične infrastrukture, ki vplivajo na varovanje informacij in informacijskih sistemov, se mora informacijska varnostna politika nenehno prilagajati z uvajanjem novih in dopolnjevanjem že obstoječih varnostnih ukrepov in postopkov.

Vsebino dokumenta knjižnica prilagodi svojim razmeram, pri določanju potrebnih kontrol pa upošteva tudi kontrole po standardu ISO/IEC 27001:2022.

Umetna inteligenca (UI)

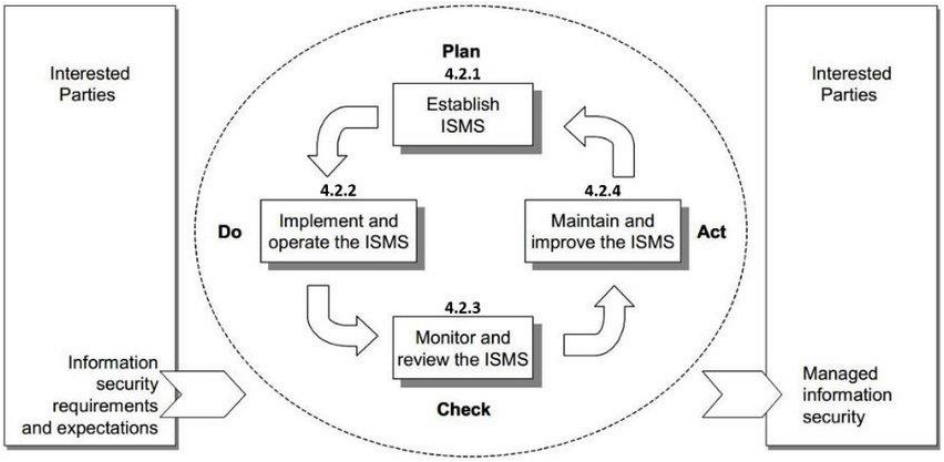
Poleg vseh definicij in orodij informacijske varnosti, ki jih bodo v obliki navodil, postopkov in obrazcev, namenjenih za izvajanje varnostne politike, knjižnice v praksi pripravile in upoštevale, se odpira precej novo področje, umetna inteligenca. Uporaba umetne inteligence šele v tem času pridobiva pravne okvirje in dokumente, ki to področje urejajo.

1. 8. 2024 je pričela veljati Uredba Evropske unije o umetni inteligenci (https://eur-lex.europa.eu/legal-content/SL/TXT/HTML/?uri=OJ:L_202401689), na kratko Akt o umetni inteligenci, kot prvi dokument takšnega tipa na svetu. Na voljo je tudi standard, ki ureja zahteve s področja umetne inteligence: ISO/IEC 42001:2023 Informacijska tehnologija – Umetna inteligenca – Sistem upravljanja umetne inteligence

Obvladovanje tega področja v širši uporabi je za knjižnice precej novo in vezano na posamezne splošne praktične rešitve. Prakse z drugih področij dela kažejo, da bo treba tudi delo na področju informacijsko komunikacijske tehnologije preoblikovati in slediti ponudbi in zahtevam, ki se z uporabo UI oblikujejo. Upravljavci tega področja bodo morali poznati ključno zasnovo UI, vzpostaviti kontrole in mehanizme upravljanja, skrbeti za skladnost z zakonodajo tega področja, prepoznati tveganja in upoštevati etične politike za to področje. Pričakujemo lahko več pravnih in zavezujočih dokumentov za posamezna področja, ki se bodo izoblikovali med širjenjem ponudbe rešitev z UI. Do takrat je treba slediti Uredbi in standardom.

Vzdrževanje in posodabljanje krovne in področnih informacijskih varnostnih politik

Aktualnost krovne informacijske varnostne politike in področnih varnostnih politik ter skladnost s spremembami informacijskega sistema upravljamo z modelom PDCA kroga.



Slika 2: Model PDCA uporabljen za procese sistema upravljanja informacijske varnosti (Vir: ISO 27001:2005)

1. Načrtovanje krovne in področnih informacijskih varnostnih politik (Plan)
2. Izvajanje in upravljanje zahtev krovne in področnih informacijskih varnostnih politik (Do)
3. Preverjanje uspešnosti izvajanja s pomočjo spremljanja, merjenj in pregledov (Check)
4. Ukrepanje s preventivnimi in korektivnimi ukrepi ter izboljšavami in posodobitvami (Act)

Uporaba krovne informacijske varnostne politike

Krovna informacijska varnostna politika s podrednim dokumentom, ki natančneje opredeljuje organizacijo upravljanja informacijske varnosti je namenjena vsem splošnim knjižnicam. Krovni dokument je oblikovan za vse knjižnice, ne glede na velikost. Posamezne varnostne politike splošna knjižnica prilagodi obsegu delovanja lastnega informacijskega sistema, z upoštevanjem osnovnih določil, ki so določena v posameznem dokumentu.
Splošna knjižnica določi datum začetka veljavnosti svoje krovne informacijske varnostne politike in celotni dokument ali njegov povzetek objavi na lastni spletni strani.
Krovno informacijsko varnostno politiko in posamezne varnostne politike je treba redno posodabljati glede na zakonska in druga določila s področja informacijske varnosti.

Definicije:

- Podatek: *dejstvo, ki o določeni stvari kaj pove ali se nanjo nanaša (Fran: https://www.fran.si/iskanje?View=1&Query=podatek)*
  Podatki sami po sebi nimajo določenega pomena, dokler jih ne razložimo (http://colos.fri.uni-lj.si/eri/INFORMATIKA/Podatki_in_informacije/podatek_informacija.html)
- Informacija je obdelan podatek
- Informacijski sistem: Informacijski sistem je množica komponent, ki sodelujejo pri zbiranju, shranjevanju, manipulaciji in porazdelitvi informacij.(http://mrvar.fdv.uni-lj.si/sola/info2/infosist/INFOSIST.PDF)
- Informacijska varnostna politika: je dokument, ki izraža odnos upravljalca do podatkov, s katerimi upravlja (https://inovis.si/informacijska-varnostna-politika-ivp/)
- ISMS (Information Security Management System): sistem upravljanja informacijske varnosti
- PDCA ali Demingov krog: »Plan-Do-Check-Akt« ali »Planiraj-Izvedi-Preveri-Ukrepaj«
- Informacijska in kibernetska varnost (https://www.info-hisa.si/kibernetska-ali-informacijska-varnost/)
- Informacijska varnost (https://www.gov.si/teme/informacijska-varnost/)
- Kibernetska varnost (https://www.microsoft.com/sl-si/security/business/security-101/what-is-cybersecurity)

Seznam virov s področja informacijske varnosti

Zakoni:

- Zakon o knjižničarstvu (ZKnj-1A), (Uradni list RS, št. 92/15 z dne 4. 12. 2015) http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO2442
- Zakon o varstvu osebnih podatkov (ZVOP-2), (Uradni list RS, št. 163/22) http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7959
- Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (zadnje dopolnitve ZVDAGA-A, Uradni list RS, št. 51/14 z dne 7. 7. 2014) http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO4284
- Zakon o elektronskih komunikacijah (ZEKom-2), (Uradni list RS, št. 130/22 in 18/23 – ZDU-1O, 13.2.2023) http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO8611
- Zakon o dostopu do informacij javnega značaja (ZDIJZ), (Uradni list RS, št. 51/06 – uradno prečiščeno besedilo, 117/06 – ZDavP-2, 23/14, 50/14, 19/15 – odl. US, 102/15, 7/18 in 141/22) http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO3336
- Zakon o Informacijskem pooblaščencu (ZInfP), (Uradni list RS, št. 113/05 in 51/07 – ZUstS-A) http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO4498
- Zakon o informacijski varnosti (ZInfV) (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23) http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7707

- Kodeks ravnanja javnih uslužbencev (Uradni list RS, št. 8/01) http://www.pisrs.si/Pis.web/pregledPredpisa?id=DRUG1022

- Splošna uredba o varstvu podatkov https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.SLV&toc=OJ:L:2016:119:FULL (**GDPR** - General Data Protection Regulation)
- Uredba o informacijski varnosti v državni upravi http://www.pisrs.si/Pis.web/pregledPredpisa?id=URED7198
  Se še uporablja do pričetka uporabe podzakonskega predpisa iz novega 18.a člena Zakona o informacijski varnosti (glej Zakon o spremembah in dopolnitvah Zakona o informacijski varnosti (Uradni list št. 49/23)).
- Uredba Evropske unije o umetni inteligenci (https://eur-lex.europa.eu/legal-content/SL/TXT/HTML/?uri=OJ:L_202401689) (na kratko Akt o umetni inteligenci)

Standardi:

- ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements
- SIST ISO/IEC 27001:2013 (sl) Informacijska tehnologija – Varnostne tehnike - Sistemi upravljanja informacijske varnosti - Zahteve
- ISO/IEC 42001:2023 Information technology - Artificial intelligence - Management system

Diplomska in magistrska dela:

- Ambrožič, Č. Knjižnice in zagotavljanje informacijske varnosti v elektronskem okolju : magistrska naloga / Črt Ambrožič. - Novo mesto : [Č. Ambrožič], 2017. - 124 str., [51] str. pril. : ilustr. ; 31 cm. - Dostopno tudi na: http://revis.openscience.si/IzpisGradiva.php?id=5024
- Rakovec, S. Varovanje informacij skladno s standardom BS 7799 : magistrsko delo / Sašo Rakovec. - Ljubljana : [S. Rakovec], 2005. - X, 92 str., 81 str. pril. : graf. prikazi ; 30 cm. - Dostopno tudi na: http://www.cek.ef.uni-lj.si/magister/rakovec543.pdf. - Dostopno tudi na: https://repozitorij.uni-lj.si/IzpisGradiva.php?id=6765
- Sirk, I. Uvajanje standardov s področja informacijske tehnologije v Mariborski knjižnici : diplomsko delo univerzitetnega študija Organizacijska informatika / Irena Sirk. - Kranj : [I. Sirk], 2013. - 112 f. : ilustr. ; 30 cm. - Dostopno tudi na: http://dkum.uni-mb.si/Dokument.php?id=55480. - Dostopno tudi na: https://dk.um.si/IzpisGradiva.php?id=40515
- Tršelič, T. Priprava strokovnih podlag za uvedbo sistema za upravljanje informacijske varnosti: diplomsko delo visokošolskega strokovnega študija Organizacija in management delovnih procesov / Tugomir Tršelič. - Kranj : [T. Tršelič], 2014. - 73 f. : ilustr. ; 30 cm. - Dostopno tudi na: https://dk.um.si/Dokument.php?id=63051&lang=slv. - Dostopno tudi na: https://dk.um.si/IzpisGradiva.php?id=44069

Članki:

- Bojanc, R. Kvantitativni model za upravljanje informacijskovarnostnih tveganj. V: Uporabna informatika (Ljubljana, Tiskana izd.). - ISSN 1318-1882. - Letn. 20, št. 2 (apr./maj/jun. 2012), str. 82-98. - Dostopno tudi na: http://www.dlib.si/details/URN:NBN:SI:doc-C6OVYLX9
- Brezavšček, A., Moškon, S. Vzpostavitev sistema za upravljanje informacijske varnosti v organizaciji. V: Uporabna informatika (Ljubljana, Tiskana izd.). - ISSN 1318-1882. - Letn. 18, št. 2 (2010), str. 101-108. - Dostopno tudi na: https://dk.um.si/IzpisGradiva.php?id=52420. - Dostopno tudi na: http://www.dlib.si/details/URN:NBN:SI:doc-HMQQRLCH
- Prešeren, T., Bajec, M. Celovit pristop obvladovanja mobilnih naprav. V: Uporabna informatika (Ljubljana, Tiskana izd.). - ISSN 1318-1882. - Letn. 17, št. 4 (okt./nov./dec. 2009), str. 255-264. - Dostopno tudi na: http://www.dlib.si/details/URN:NBN:SI:doc-WNR3N2KR

Razno:

- Krovna informacijska varnostna politika. Univerza v Mariboru, 2013. – Dostopno tudi na: https://it.um.si/varnostna-politika/Documents/Krovna%20informacijska%20varnostna%20politika.pdf . - Dostopno tudi na: https://it.um.si/varnostna-politika/strani/informacijska-varnostna-politika.aspx
- Informacijska varnostna politika za področje informacijsko-komunikacijske tehnologije (IKT). Univerza v Mariboru, 2013. - Dostopno tudi na: https://it.um.si/varnostna-politika/Documents/Informacijska%20varnostna%20politika%20za%20podro%C4%8Dje%20informacijsko-komunikacijske%20tehnologije%20(IKT).pdf
  Dostopno tudi na: https://it.um.si/varnostna-politika/strani/informacijska-varnostna-politika.aspx
- Islovar: terminološki slovar informatike. Slovensko društvo Informatika, c. 2020. http://islovar.org/islovar/islovar
- Temeljni pojmi: informatika. Arnes, 2015. https://informatika-tretja.splet.arnes.si/files/2015/04/Temeljni-pojmi.pdf
- Etične smernice za uporabo umetne inteligence in podatkov pri poučevanju in učenju za izobraževalce https://op.europa.eu/sl/publication-detail/-/publication/d81a0d54-5348-11ed-92ed-01aa75ed71a1
- Praktična uporaba umetne inteligence v knjižnicah / Artificial Intelligence Solutions in Libraries https://www.youtube.com/watch?v=xrgXFdgnnvA
- Priložnosti in pasti uporabe metod umetne inteligence https://www.youtube.com/live/r95islitd_M
- Portal IVARNOST.SI https://ivarnost.si/
- MiPi : medijska in informacijska pismenost Agencije za komunikacijska omrežja in storitve Republike Slovenije https://www.mipi.si/